INVESTIGATION OF PRIMARY SCHOOL TEACHERS’ CYBER RESILIENCE LEVELS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

BORAN KOCA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
COMPUTER EDUCATION AND INSTRUCTIONAL TECHNOLOGY

JUNE 2025

Approval of the thesis:

INVESTIGATION OF PRIMARY SCHOOL TEACHERS' CYBER RESILIENCE LEVELS

submitted by **BORAN KOCA** in partial fulfillment of the requirements for the degree of **Master of Science in Computer Education and Instructional Technology, Middle East Technical University** by,

Prof. Dr. Naci Emre Altun
Dean, **Graduate School of Natural and Applied Sciences** ________________

Prof. Dr. Soner Yıldırım
Head of the Department, **Computer and Instructional Technology Education** ________________

Prof. Dr. Ömer Delialioğlu
Supervisor, **Computer and Instructional Technology Education, METU** ________________

Assoc. Dr. Aslıhan İstanbullu
Co-Supervisor, **Computer and Instructional Technology Education, Amasya University** ________________

Examining Committee Members:

Prof. Dr. Hasan Çakır
Computer Edu. & Inst. Tech., Gazi University ________________

Prof. Dr. Ömer Delialioğlu
Computer Education and Instructional Technology, METU ________________

Assoc. Prof. Dr. Erkan Er
Computer Education and Instructional Technology, METU ________________

Date: 13.06.2025

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name Last name : Boran Koca

Signature :

ABSTRACT

INVESTIGATION OF PRIMARY SCHOOL TEACHERS' CYBER RESILIENCE LEVELS

Koca, Boran
Master of Science, Computer Education and Instructional Technology
Supervisor : Prof. Dr. Ömer Delialioğlu
Co-Supervisor: Assoc. Prof. Dr. Aslıhan İstanbullu

13 June 2025, 125 pages

This study aims to examine the cyber resilience levels of primary school teachers within the context of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and their relationship with demographic and behavioral traits such as experience, duration of daily internet use, and whether they had received previous cybersecurity training. A total of 192 primary school teachers were surveyed online, and a cross-sectional quantitative design was employed. The cyber resilience of the teachers was assessed through open-ended questions aligned with CSF in a cyber-attack scenario form. Using a rubric, qualitative data were converted into quantitative data. After measuring validity with Cohen's Kappa, data were analyzed using descriptive and non-parametric statistics.

The findings showed that teachers' cyber resilience skills need improvement in terms of the five functions of the NIST CSF. Separate analysis of the sub-factors confirmed that they also need improvements in the fields of maintaining a safe school environment, including recognizing risky data, identifying problems, resisting threats, and recovering from attacks. According to the distributions, they have the necessary knowledge and skills in protection functions, i.e., simple proactive security measures. There is a statistically significant difference in teachers' cyber resilience with respect to gender. The use of digital tools has a slight positive correlation with the total cyber resilience scores. Neither the daily internet usage time factor nor the professional experience factor has any significant relationship with teachers' cyber resilience. On the other hand, the factor of receiving cybersecurity training has a significant impact on teachers' cyber resilience. This study contributes to the development of training programs for teachers to enhance their cyber resilience skills and thus to create a safer school environment.

Keywords: Cyber Threats, Cybersecurity, Cyber Resilience, Cyber Attacks, Primary School Teachers

ÖZ

İLKOKUL ÖĞRETMENLERİNİN SIBER DAYANIKLILIKLARININ SİBER SEVİYELERİNİN İNCELENMESİ

Koca, Boran
Yüksek Lisans, Bilgisayar ve Öğretim Teknolojileri Eğitimi
Tez Yöneticisi: Prof. Dr. Ömer Delialioğlu
Ortak Tez Yöneticisi: Assoc. Prof. Aslıhan İstanbullu

13 Haziran 2025, 125 sayfa

Bu çalışma, ilkokul öğretmenlerinin Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Siber Güvenlik Çerçevesi (CSF) bağlamındaki siber dayanıklılık düzeylerini ve bu düzeylerin deneyim, günlük internet kullanım süresi ve daha önce siber güvenlik eğitimi alıp almadıkları gibi demografik ve davranışsal özelliklerle ilişkisini incelemeyi amaçlamaktadır. Toplam 192 ilkokul öğretmeni çevrim içi anketle çalışmaya katılmış ve kesitsel nicel bir araştırma deseni uygulanmıştır. Öğretmenlerin siber dayanıklılıkları, bir siber saldırı senaryosu formunda CSF ile uyumlu açık uçlu sorular aracılığıyla değerlendirilmiştir. Nitel veriler, bir dereceli puanlama anahtarı (rubrik) kullanılarak nicel verilere dönüştürülmüştür. Cohen's Kappa ile geçerlik ölçümünün ardından veriler betimsel ve parametrik olmayan istatistiklerle analiz edilmiştir.

Bulgular, öğretmenlerin NIST CSF'nin beş işlevi bağlamında siber dayanıklılık becerilerinin geliştirilmesi gerektiğini göstermektedir. Alt faktörlerin ayrı ayrı analizinde, öğretmenlerin riskli verileri tanıma, sorunları belirleme, tehditlere karşı direnme ve saldırılardan kurtulma gibi alanlar da dahil olmak üzere güvenli bir okul ortamını sürdürme konusunda da gelişime ihtiyaç duydukları doğrulanmıştır. Dağılımlar incelendiğinde, koruma işlevleri yani basit önleyici güvenlik önlemleri konusunda gerekli bilgi ve becerilere sahip oldukları görülmektedir. Öğretmenlerin siber dayanıklılık düzeyleri cinsiyete göre istatistiksel olarak anlamlı bir farklılık göstermektedir. Dijital araç kullanımının, toplam siber dayanıklılık puanları ile hafif düzeyde pozitif korelasyonu bulunmaktadır. Günlük internet kullanım süresinin anlamlı bir farkı ya da mesleki deneyim faktörünün öğretmenlerin siber dayanıklılığı ile anlamlı bir ilişkisi bulunmamaktadır. Öte yandan, siber güvenlik eğitimi alma faktörü öğretmenlerin siber dayanıklılığı üzerinde anlamlı bir etkiye sahiptir. Bu çalışma, öğretmenlerin siber dayanıklılık becerilerini geliştirmeye yönelik eğitim programlarının oluşturulmasına ve dolayısıyla daha güvenli bir okul ortamı sağlanmasına katkıda bulunmaktadır.

Anahtar Kelimeler: Siber Tehditler, Siber Güvenlik, Siber Dayanıklılık, Siber Saldırılar, İlkokul Sınıf Öğretmenleri

Dedicated to my family and friends

ACKNOWLEDGMENTS

I want to express my sincere gratitude to the individuals and institutions that contributed to the completion of this thesis.

I would like to express my deepest gratitude to Prof. Dr. Ömer DELİALİOĞLU for his invaluable guidance, expertise, and encouragement throughout this research journey. His insights were crucial in shaping this study. I am equally grateful to my co-supervisor, Assoc. Prof. Dr. Aslıhan İSTANBULLU, for her important contributions, insightful suggestions and unwavering support that greatly enriched this study.

Finally, I would like to express my deepest gratitude to all the primary school teachers who generously gave their time and shared their valuable perspectives and ideas. Without their participation and cooperation, this research would not have been possible.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

ABBREVIATIONS

Amazon Web Services (AWS)

Bring Your Own Device (BYOD)

Cybersecurity and Infrastructure Security Agency (CISA)

Control Objectives for Information and Related Technologies (COBIT)

Cyber Resilience Story Form for Teachers (CRSFT)

Cybersecurity Framework (CSF)

Department for Science, Innovation and Technology (DSIT)

Educational Informatics Network (EIN)

Federal Trade Commission (FTC)

Higher Education Institution (HEI)

Human Research Ethics Committee (IAEK)

International Business Machines (IBM)

Information and Communication Technology (ICT)

Information Systems Audit and Control Association (ISACA)

Information Security Management System (ISMS)

International Organization for Standardization (ISO)

International Electrotechnical Commission (IEC)

Internet of Things (IoT)

Information Technology (IT)

National Academies of Science (NAS)

National Institute of Standards and Technology (NIST)

Organization of American States (OAS)

Optical Character Recognition (OCR)

Operational Technology (OT)

Personally Identifiable Information (PII)

Pacific Northwest National Laboratory (PNNL)

Request for Information (RFI)

Supply Chain Risk Management (SCRM)

United States Government (USAGov)

World Economic Forum (WEF)

CHAPTER 1

INTRODUCTION

This chapter features detailed information about the study's background, problem statement, purpose, and significance, research questions, definitions of terms, and chapter summary.

1.1 Background of Study

Rapid digitalization has fundamentally altered the educational landscape, transforming schools into increasingly vulnerable targets for cyber threats (Nugroho, Afiana, & Kuncoro, 2024; Internet Crime Complaint Center, 2018). Educational institutions, holding sensitive data like student and teacher records, often face cyberattacks due to limited security resources and budget constraints (Ronen, 2024). Statistics highlight the severity of this issue: the Verizon Business Report (2023) places education among the top five sectors targeted by ransomware, noting an average of 1,780 weekly cyberattacks and a 258% increase in overall incidents in 2023. Check Point reports indicate a consistent rise in attacks on educational institutions (Check Point Software Technologies Ltd., 2022), with the sector facing the highest average weekly attacks globally in 2023 (2,046), exceeding government and healthcare (Check Point, 2024). Emsisoft Malware Lab (2023) notes a doubling in attacks directly affecting K-12 schools. Threats vary, with phishing and spam accounting for 40% of emails to educational accounts, often leading to breaches via compromised credentials (Sophos, 2024). These vulnerabilities result in significant data breaches, financial losses, disruption of services, and reputational damage (Bouke, Abdullah, Hamoud, Zaid, & El Atigh, 2023).

Effectively addressing cyber threats requires more than technical measures; it depends significantly on teachers' cybersecurity awareness and resilience. Teachers must integrate security into their teaching and update their knowledge on threats and protection methods (Petruzzelli & Sharma, 2019; Yan, Xue, & Lou, 2021). However, research indicates a concerning lack of preparedness, with a significant percentage of teachers in the US and UK reporting no recent cybersecurity training (Clever, 2023; Department for Science, Innovation and Technology [DSIT], 2024). Many teachers in Türkiye also feel insufficient in cybersecurity and digital literacy (Altınöz, Tosun, Çinkılıç & Çay, 2019). Cyberattacks weaken teachers' confidence, cause stress and burnout, and disrupt educational services (Gu & Day, 2013; Akor, Nongo, Udofot & Oladokun, 2024).

Cybersecurity knowledge is also crucial for students. While digitally fluent, many students lack the skills to cope with cyber threats (Akor vd., 2024). Online risks can harm data integrity, digital citizenship, and socio-emotional well-being (Carvalho, Carvalho, Silva, Santos, & Bandeira, 2023). Teachers must therefore guide students in safe and conscious digital use (Akor vd., 2024; Tazi, Shrestha, Norton, Walsh, & Das, 2021). Fostering student resilience in the digital world is thus linked to increasing teacher cyber resilience.

Cyber resilience, distinct from traditional cybersecurity, is defined as an organization's ability to minimize the impact of significant cyber incidents on its objectives (World Economic Forum [WEF], 2024) or the capacity to continuously deliver desired outcomes despite adverse cyber events (Björck, Henkel, Stirna, & Zdravkovic, 2015). It acknowledges that incidents will occur and emphasizes anticipating, withstanding, recovering from, and adapting to events (National Institute of Standards and Technology, 2018; Linkov, Eisenberg, Plourde, Yatsalo, & Kott, 2013; Alshar'e, 2023). Control Objectives for Information and Related Technologies(COBIT), International Organization for Standardization(ISO) 27001, and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) provide structured approaches for managing cyber risk and enhancing resilience. NIST CSF defines cyber resilience through five core functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2024). For teachers, these functions involve knowing what data needs protection (Identify), taking preventive measures like strong passwords (Protect), recognizing a cyber event (Detect), reporting incidents (Respond), and restoring data/systems after an event (Recover).

Considering the increase in attacks on educational institutions (Check Point, 2022) and the increasing importance of teachers' cyber resilience (Altınöz et al., 2019), whether primary school teachers can individually implement NIST CSF targets in K-12 environments will guide future research and planning to determine the applicability and effectiveness of the framework (Alshar'e, 2023). However, according to the literature, there is a lack of data on educators' experiences and capabilities related to the five NIST CSF functions. Thus, providing aid to increase cyber resilience in schools is difficult. Therefore, the study aims to address the literature gap by examining primary school teachers’ awareness of cyber threats, current readiness, and capacity to handle cybersecurity issues. Accordingly, it was planned to measure cyber resilience by developing a scenario-based survey that explicitly examines how the five core functions of the NIST CSF are scored in terms of cyber resilience. The aim is to provide a safer learning environment per the observations made. In this context, inferences will be made to help create cyber resilience teaching materials, policy guidelines, and training modules.

1.2 Cyber Resilience and NIST Cybersecurity Framework (CSF)

Cyber resilience is becoming popular because, with its broad scope and individual perspective, it offers more guaranteed solutions against cyberattacks. Organizations such as the World Economic Forum [WEF] (2024) have also defined cyber resilience as the capacity to continue an organization's basic operations and values after major cyberattacks while reducing the adverse effects on resources. In addition, Björck et al. (2015) defined this concept as the capacity to continue operations and reliably produce the intended result despite cyber threats and their adverse effects.

Unlike cybersecurity, one of the most distinctive features of cyber resilience is the acceptance that absolute security is impossible to achieve (Linkov & Kott, 2018). According to Björck et al. (2015), unlike cyber security, this concept does not only aim to eliminate cyberattacks ("fail-safe"); in addition, it aims to overcome the threat most harmlessly, to gain the ability to recover from the attack, and to return to the old operations in the shortest time ("safe-to-fail"). According to the definitions of institutions such as the National Institute of Standards and Technology (NIST) and the National Academies (NAS), cyber resilience is the ability to predict cyber-attack events, withstand their effects, recover from them, and adapt to changing threat conditions (National Institute of Standards and Technology, 2018; Linkov et al., 2013; Alshar'e, 2023). In other words, the recoverability of the system, the continuity of operation, the feeling of security of users, and the ability to learn and grow from what you learn (Tzavara & Vassiliadis, 2024). Various frameworks and recommendations have been developed to operationalize and strengthen cybersecurity. The National Institute of Standards and Technology Cybersecurity Framework, developed by the United States, is one of the best-known frameworks, along with COBIT and ISO27001. As it is shown in Figure 1.1, through its five main functions, NIST CSF offers a structured method for managing cybersecurity risks:

Identify: Recognize that systems, users, data, and operations may be exposed to cyber threats. Educators must understand what personal information or teaching materials must be protected.

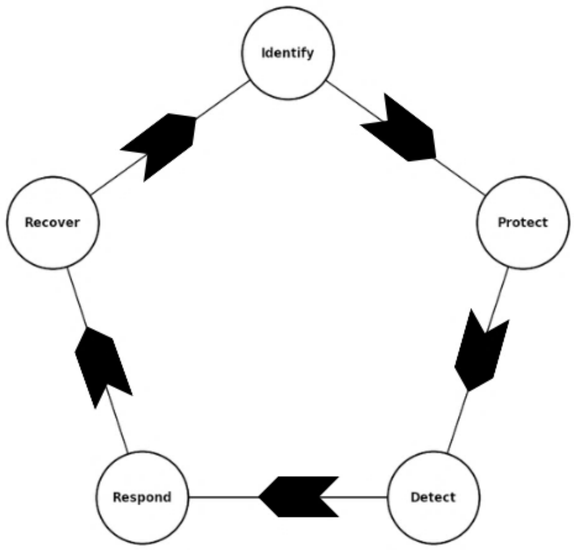
Protect: Actively use appropriate security mechanisms to protect critical services. Examples include password protection for accounts in applications and antivirus software.

Detect: Detect if a cyber-attack has occurred by knowing, following, and implementing procedures. This may involve identifying signs of computer viruses or phishing attacks.

Respond: Act upon recognition of a cybersecurity incident. For a teacher, this may involve not disrupting the lesson and reporting a suspected attack to IT or school staff after the lesson.

Recover: Follow procedures to restore interrupted operations, lost information, or damaged applications due to a cybersecurity incident. If an incident occurs, this may require data recovery from backups.

Universities and other organizations can use the NIST CSF to assess their cybersecurity attitudes in a systematic manner using standard terminology.



(NIST, 2018)

Figure 1.1 NIST Cybersecurity Framework Core Functions

1.3 Problem Statement

Primary school teachers play a crucial role in shaping the digital citizenship of their students; therefore, they have the potential to influence society through their students (Amankwa, 2021). In addition, primary school children are a remarkable group because the weakest link in cybersecurity is the 'human factor' (Richardson, Lewis, & Burnette, 2019). Studies reinforcing this risk show that primary school teachers' cybersecurity awareness levels are 'not at the desired level and are even lacking, especially in technical competence and responsibility areas (Canoğulları, 2021; Wang, Mosher & Duett, 2024). The fact that they generally do not have special specialized training in the field of cybersecurity also leaves them more vulnerable to threats

(Malecki, 2018). Moreover, despite teaching digital citizenship and being knowledgeable about cybersecurity concepts, teachers often lack adequate preparation for cyber incidents (Petruzzelli & Sharma, 2019; Tazi et al., 2021). Additionally, most educators in various countries reported not receiving cybersecurity training; for instance, 26% of teachers in the United States reported having no cybersecurity training (Clever, 2023). According to research, in the United Kingdom, 38% of primary schools and 25% of secondary schools are known to have had no cybersecurity training or awareness activities in the previous 12 months (DSIT, 2024). Moreover, unfortunately, many teachers report being concerned about digital security and feeling unprepared for cyber threats (Altınöz et al., 2019). Similarly, studies conducted in Türkiye have shown a widespread inadequacy among teachers in cybersecurity and digital literacy (Altınöz et al., 2019). Their cyber resilience levels frequently fail to meet the demands of the modern digital world (Wohlfart & Wagner, 2023). In parallel with these findings, studies have shown that when such situations occur, this gap can create stress, erode educators' self-confidence, and disrupt the educational process (Gu & Day, 2013; Akor et al., 2024). This inadequacy leaves them and the data they manage particularly vulnerable to common attacks such as phishing and social engineering (Malecki, 2018).

This deficiency is particularly critical at the primary school level. Primary school teachers directly impact on the institution's overall security posture because they directly manage sensitive student data such as personal identification information, health records, and academic progress; in addition, they are the first line of defense and primary gatekeeper in the institution's cybersecurity chain as they oversee digital interactions in the classroom (Amankwa, 2021; Richardson et al., 2019). Additionally, primary school teachers serve as role models when students are introduced to the digital world and develop basic digital habits. Teachers not only impart academic knowledge but also shape the cyber resilience of future generations by modeling safe, responsible, and ethical digital behaviors for them (Kuş & Mert, 2024). Therefore, teachers' cyber resilience also impacts students' cyber safety.

Currently, frameworks such as NIST CSF provide detailed guidance for managing school cybersecurity risks. On the other hand, this deficiency cannot be addressed despite the existence of established frameworks, as extra attention is needed to operationalize this framework in the K-12 classroom environment and to adapt it to this delicate environment (Alshar'e, 2023). There is a lack of data on the experience, knowledge, and ability of K-12 teachers to fulfill the five basic NIST CSF functions. In addition, regarding cyber resilience, it is unclear whether teachers are aware of the appropriate actions to take against the cyber threats they encounter and need to address in their daily work lives. Thus, this lack of information makes it more challenging to develop professional development training and specific intervention guidelines for cyber resilience in these situations. Efforts to integrate cybersecurity into schools will remain generic and less effective unless teachers' cyber resilience dimensions, strengths, and weaknesses are clearly analyzed.

1.4 Purpose of the Study

Undoubtedly, cyberattacks targeting educational institutions are significantly increasing. Indeed, research highlights this alarming trend (Internet Crime Complaint Center, 2018). Recent reports confirm this growing threat landscape (Verizon Business, 2023). Furthermore, security analyses demonstrate the escalation of such attacks (Check Point, 2024). Therefore, this study aims to analyze primary school teachers' cyber resilience perceptions. Research indicates inadequate cybersecurity knowledge (Javidi & Sheybani, 2018; Clever, 2023). Similarly, government reports identify serious gaps in educator preparedness (DSIT, 2024). Moreover, academic studies confirm this training deficit (Petruzzelli & Sharma, 2019). Likewise, related research highlights this critical shortcoming (Tazi et al., 2021). Teachers' readiness to face cyber threats will be assessed in that case. Additionally, their capacity to effectively respond to cybersecurity challenges during their professional practices will be investigated.

The study is based on the five core functions of NIST CSF (National Institute of Standards and Technology, 2018). These functions are specifically Identify, Protect, Detect, Respond, and Recover (Alshar'e, 2023). Specifically, this framework offers a structured approach to cybersecurity assessment (NIST, 2024). Then, teachers' cyber resilience competencies will be assessed and scored according to these functions (RQ1). Therefore, this approach will measure both proactive and reactive characteristics of cyber resilience, encompassing basic cybersecurity, cyber awareness, and cyber literacy knowledge. As a result, it will measure the behaviors and reactions of educators in the most critical situations encountered in daily life, identifying strengths, weaknesses, and areas for improvement. These will indicate the key points to focus on and the areas to concentrate on for the training to be provided.

Moreover, studies in the literature focusing on cyber awareness, cyber literacy, and cybersecurity among teachers have examined factors such as gender, internet usage time, screen time, years of professional experience, and whether individuals have received training on the subject to measure the effects of daily behaviors, experiences, and upbringing. This study aims to conduct an exploratory analysis of factors that may affect the cyber resilience of primary school teachers (RQ2). Indeed, previous studies suggest that various factors influence preparedness and behavior. For instance, research indicates cybersecurity training significantly impacts awareness (Altınöz et al., 2019). Similarly, educational reports highlight the importance of proper training (Clever, 2023). In addition, government documents emphasize training adequacy (DSIT, 2024). Likewise, international studies confirm training's role in preparedness (Sapanca & Kanbul, 2022). Furthermore, technology use behaviors may relate to resilience levels (Akor et al., 2024). Also, research links the frequency of digital tools to security awareness (Chou & Chou, 2016). Besides, studies connect internet use patterns with cybersecurity behaviors (Sapanca & Kanbul, 2022). In this context, demographic factors will be examined. Separately, years of teaching experience will be examined. Furthermore, professional factors such as whether they have received prior cybersecurity training will also be collected. Additionally, it will determine whether there are relationships between technology adoption behaviors and cyber resilience levels.

In summary, the purpose of this study is to provide empirical data on primary school teacher cyber resilience using the NIST CSF framework. Consequently, new methods to support more focused and successful interventions will be suggested based on the findings. Ultimately, the research hopes to make a contribution to the literature on cyber resilience in K-12 educators. Finally, it aims to inform efforts to design and develop more secure online learning environments for educators and students.

1.5 Research Questions

RQ1: What are the descriptive statistics (e.g., mean, standard deviation, and median) for teachers' overall cyber resilience scores and each of their five sub-dimensions?

RQ2: To what extent, if any, do teachers' overall cyber resilience scores differ based on the following demographic and professional characteristics?

> **RQ2a:** What is the difference in cyber resilience scores between teachers of different genders?
>
> **RQ2b:** What is the difference in cyber resilience scores between teachers who have received cybersecurity training and those who have not?
>
> **RQ2c:** What is the difference in cyber resilience scores between the duration of daily internet usage?
>
> **RQ2d:** What is the relationship between the frequency of digital tool use and teachers' cyber resilience scores?
>
> **RQ2e:** What is the relationship between years of professional experience and teachers' cyber resilience scores?

1.6 Significance of Study

Cyber threats against schools are escalating and severe (Verizon Business, 2023; Check Point, 2024). Consequently, teachers play a critical role in these digital environments (Petruzzelli & Sharma, 2019). Therefore, understanding and enhancing teacher cyber resilience is paramount (Yan et al., 2021). Indeed, research consistently shows many teachers lack adequate training (Altınöz et al., 2019; Clever, 2023; DSIT, 2024). As a result, they often feel unprepared for incidents (Akor et al., 2024). In that case, this lack of preparedness can disrupt education services. Furthermore, it can negatively impact teacher well-being (Gu & Day, 2013; Akor et al., 2024). Moreover, teachers guide students in digital practices. Thus, teacher resilience is linked to fostering student cyber resilience (Akor et al., 2024; Tazi et al., 2021).

Notably, the NIST Cybersecurity Framework (CSF) offers a structured approach. Specifically, it helps manage cyber risks and enhance resilience (National Institute of Standards and Technology, 2018; Alshar'e, 2023). In particular, it covers five core functions: Identify, Protect, Detect, Respond, and Recover. However, there is a notable gap in research. Specific analysis on how primary teachers apply these standards is missing (Alshar'e, 2023). Additionally, data is needed on educators' capabilities within these NIST CSF functions (Altınöz et al., 2019). Hence, this study directly addresses this gap. Primarily, it examines primary teacher cyber resilience using the NIST CSF (RQ1). Moreover, it investigates how demographic and behavioral factors relate to these levels (RQ2).

Undoubtedly, the study's findings offer significant, data-driven contributions. Subsequently, they provide actionable insights for various stakeholders. For instance, for teachers, results will highlight areas for improvement. Particularly, this is true for recognizing threats and protective measures (Totseva, 2024). As such, it increases their awareness and ability to protect themselves and their students. Similarly, for school administrators and IT personnel, the data helps evaluate staff security posture. Accordingly, it supports resource planning and tailored policies (Yousif Yaseen, 2022). Likewise, the research gives evidence for policymakers and curriculum developers. Consequently, this supports integrating NIST CSF content into training. Therefore, it advocates for structured, mandatory programs. However, some might argue that informal learning could also be effective. Ultimately, this study provides detailed, framework-based insights. Finally, these enable more targeted interventions. Indeed, this helps create safer digital learning environments for everyone.

1.7 Definition of Key Terms

Classroom Teachers: Public school teachers in the K-12 system, from kindergarten to 5th grade.

Cyber Attacks: Intended to steal, alter, or destroy digital data; also, intentional actions to disrupt services or gain unauthorized access. They target computer operating systems, infrastructure, networks, or personal devices (Sophos, 2024). For example, they aim to disrupt services, gain unauthorized access, or steal, alter, or destroy data (Bouke et al., 2023).

Cyber Resilience: The ability of individuals and systems to maintain essential functions in the face of cyberattacks (National Institute of Standards and Technology, 2018; Linkov et al., 2013; Alshar'e, 2023). It involves minimizing negative impacts and learning from experience (Björck et al., 2015). The steps of this ability are to anticipate, withstand, recover from, adapt to, and recover from cyber threats (Alshar'e, 2023).

Cybersecurity: The function of systems, networks, and programs to protect against cyberattacks. The protection of sensitive information, prevention of digital theft, or disruption of cyberattacks (Linkov ve Kott, 2018).

Cyber Threats: These are situations that can damage important data, cause it to be stolen, and are carried out by hackers. They are malicious actions taken to disrupt digital operations (Sophos, 2024).

CHAPTER 2

LITERATURE REVIEW

This chapter outlines the conceptual framework of cyber resilience in terms of its scope, relationship to cybersecurity, dimensions, and importance, particularly in education. It examines specific cyber threats and security issues facing educational institutions and focuses on securing educational information. Also, it presents the current status of educators' cyber resilience in terms of their digital roles, understanding of cybersecurity issues, and levels of digital literacy. Additionally, it discusses the existing cybersecurity standards and schemes in the literature to determine their applicability to education and provides a rationale for adopting the NIST Cybersecurity Framework as a comprehensive guideline. Accordingly, it visits the historical background and explains the purpose and primary components of the NIST CSF: Identification, Protection, Detection, Response, and Recovery. Finally, it synthesizes the findings and comparisons of national and international studies on educators' cyber resilience and the distribution of researches demonstrated in the Figure 2.1.

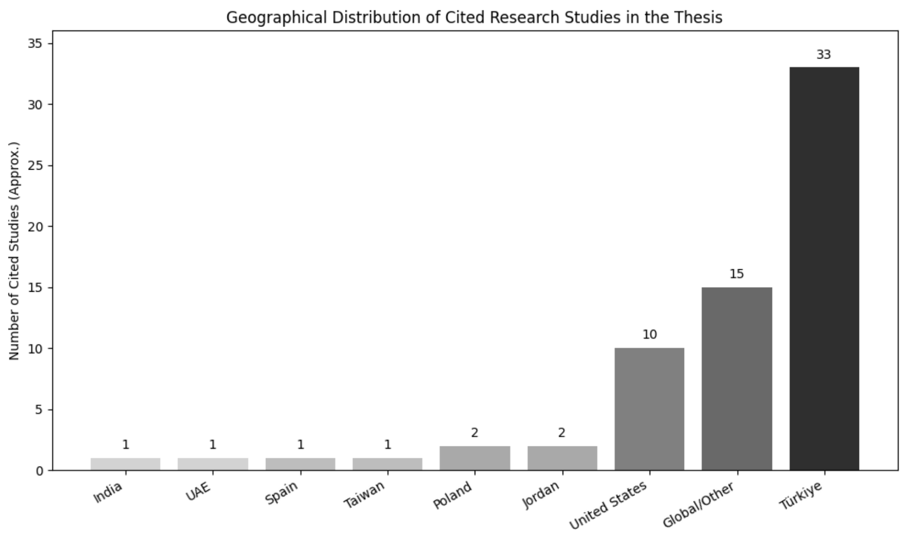


Figure 2.1 Geographical Distribution of Cited Research Studies in the Thesis

2.1 Conceptual Framework of Cyber Resilience

The prevalence and complexity of cyber risks have increased because people are now dependent on complex and interconnected digital systems and have integrated them into their lives by fully trusting them (Linkov & Kott, 2018; Al-Hawamleh, 2024). Cybersecurity measures alone are not enough to cope with unplanned, unexpected, and potentially cascading cyber threats; traditional strategies such as focusing on threat/risk assessments are also insufficient (Linkov & Kott, 2018). The inability to guarantee complete security or hardening of systems against all possible threats has led to a shift (WEF, 2024; Linkov & Kott, 2018; Tzavara & Vassiliadis, 2024). These radical changes have envisioned and developed cyber resilience as a strategic idea for public and private sector organizations (Tzavara & Vassiliadis, 2024; Pacific Northwest National Laboratory [PNNL], 2018). The following section discusses the conceptual framework of cyber resilience, including its definition, scope, relationship with cybersecurity, educational applicability, and basic dimensions.

2.1.1 Definition and Scope of Cyber Resilience

Although cyber resilience has gained widespread use and significance since the early 2000s, there is still no accepted scientific definition for the term (Smith, 2023). It has diverged dramatically from its original meaning and has been used in a wide range of fields, often to the point of becoming unintelligible or reduced to a "meaningless buzzword" (Smith, 2023; Klein, Nicholls, & Thomalla, 2004). According to the research, a lack of clarity is caused by multiple conflicting definitions, which impedes effective measurement and rigorous academic progress (Smith, 2023).

Nonetheless, cyber resilience can be conceptualized using several early definitions. Cyber resilience is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources," according to the U.S. National Institute of Standards and Technology (NIST) (Tzavara & Vassiliadis, 2024; Smith, 2023; PNNL, 2018). Organizations like the National Academies of Science (NAS) and MITRE use and refer to this definition, or variations on it that are based on rigorous adherence to the preparation, absorb, recover, and adapt processes (Linkov & Kott, 2018; Tzavara & Vassiliadis, 2024).

Other definitions emphasize the purpose or impact. For example, Björck et al. (2015) put it plainly: "the capability to continually achieve the desired impact despite negative cyber incidents." Also, the strategic definition provided by the World Economic Forum (WEF)(2024) is "the readiness of an organization to keep its core purposes and functions intact against major cyber incidents."

Cyber resilience is broad and applies to technological systems (IT systems, networks) and companies, missions, and even larger entities like nations (Björck et al., 2015; Tzavara & Vassiliadis, 2024). According to WEF (2024) and Tzavara & Vassiliadis (2024), it includes both the operational technology (OT) and information technology (IT) environments. Importantly, cyber resilience is increasingly recognized in the context of complex socio-technical systems. Moreover, it acknowledges how technology, people, processes, and larger social and cognitive domains interact (Linkov & Kott, 2018; Dunn Cavelty, Eriksen, & Scharte, 2023; Bıçakcı & Evren, 2025).

2.1.2 The Relationship Between Cyber Resilience and Cybersecurity

The definition of digital citizenship encompasses the responsible and appropriate use of technology; in other words, individuals acting in the digital world in an ideally safe, legal, and ethical manner (Brown, 2023). It provides a proactive framework that aims to teach students and educators how to be “good citizens” in the online environment (Brown, 2023). However, a fundamental limitation of digital citizenship education is that students may possess online security knowledge but are not always able to apply it in immediate situations (Brown, 2023). On the other hand, cyber resilience encompasses an individual’s ability not only to take precautions against cyberattacks but also to prepare for, resist, recover from, and adapt to these events (Linkov & Kott, 2018; Tzavara & Vassiliadis, 2024). Therefore, while digital citizenship teaches "what to do," cyber resilience focuses on "what to do when an incident occurs and learning from mistakes afterward" (Linkov & Kott, 2018).

In short, the concept of digital citizenship lays the foundation for information on proactive, responsible digital behavior examples (Brown, 2023), while cyber resilience provides the necessary reaction skills in cases where this information is insufficient or exceeded (Linkov & Kott, 2018). In this context, since teachers are perceived as possessing basic digital citizenship skills (Yılmaz, Şahin, & Akbulut, 2016; Canoğulları, 2021), the concept of cyber resilience warrants investigation.

2.1.3 The Relationship Between Cyber Resilience and Cybersecurity

Although cyber resilience has gained widespread use and importance since the early 2000s, there is still no accepted scientific definition for the term (Smith, 2023). It has strayed significantly from its original meaning and has become obscure or reduced to a “meaningless buzzword” across various fields (Smith, 2023; Klein et al., 2004). According to research, a lack of clarity results from multiple conflicting definitions; therefore, this hinders both effective measurement and rigorous academic progress (Smith, 2023).

However, cyber resilience can be conceptualized using several well-established definitions. Cyber resilience, according to the U.S. National Institute of Standards and Technology (NIST), is “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or hazards in systems that use or are enabled by cyber resources” (Tzavara & Vassiliadis, 2024; Smith, 2023; PNNL, 2018). Organizations such as the National Academies of Sciences (NAS) and MITRE build on this definition and synthesize variations of it based on strict adherence to the preparedness, absorption, recovery, and adaptation processes in the NIST CSF (Linkov & Kott, 2018; Tzavara & Vassiliadis, 2024).

Other definitions emphasize the purpose or impact. For example, as Björck et al. (2015) explicitly put it, “the ability to consistently achieve the desired impact despite adverse cyber events.” In addition, according to the strategic definition provided by the World Economic Forum [WEF] (2024), cyber resilience is "the readiness of an organization to maintain its core objectives and functions intact against major cyber incidents."

Cyber resilience is a broad concept and applies not only to technological systems, namely IT systems and networks, but also to larger entities such as companies, missions, and even nations (Björck et al., 2015; Tzavara & Vassiliadis, 2024). Therefore, it covers both operational technology (OT) and information technology (IT) environments (WEF, 2024; Tzavara & Vassiliadis, 2024).

More importantly, cyber resilience is also widely recognized in the context of complex socio-technical systems. For example, Bıçakcı and Evren (2025) call this concept cyber resilience and emphasize that each person can follow different paths within cyber threat processes. It also recognizes that technology encompasses how people, processes, and broader social and cognitive domains interact (Linkov & Kott, 2018; Dunn Cavelty et al., 2023).

2.1.4 Dimensions and Importance of Cyber Resilience

Anticipate/Prepare, Endure/Absorb, Recover, and Adapt/Evolve are the characteristics outlined by common frameworks such as NIST and NAS. It characterizes cyber resilience, a complex term (Linkov & Kott, 2018; Tzavara & Vassiliadis, 2024). According to Bıçakcı and Evren (2025), resilience is a continuously occurring process or capability rather than a static state. Key definitions include the ability to sustain the intended outcome, limiting the impact to key objectives, operating in a fail-safe mode rather than anticipating optimal prevention; moreover, the most important identified characteristics include having resilience in the face of changing conditions and threat scenarios (Björck et al., 2015; WEF, 2024; Tzavara & Vassiliadis, 2024). Traditional cybersecurity has limitations, and our dependence on increasingly complex digital infrastructures is increasing; therefore, it is imperative to ensure our cyber resilience (Linkov & Kott , 2018).

Accordingly, Al-Hawamleh (2024) and Björck et al. (2015) defined cyber resilience as the capacity to continue providing critical services and operations during and after business/operational continuity outages. It is also necessary to protect vital systems such as electricity, banking, transportation, and healthcare, i.e., "critical infrastructure protection" (PNNL, 2018; Linkov & Kott, 2018). In other words, cyber resilience is the reduction of damage, financial loss, reputational damage, and social unrest caused by cyberattacks (PNNL, 2018; WEF, 2024). In this context, protecting the nation from cyber warfare and state-sponsored attacks (PNNL, 2018; Linkov & Kott, 2018), in addition to enabling organizations to leverage digital potential and associated risks, is known as "facilitating digital transformation" (WEF, 2024). According to WEF (2024) and Al-Hawamleh (2024), cyber resilience is essentially a strategic management responsibility that requires organizational commitment, appropriate governance, and frequent stakeholder engagement. There are all challenges, such as the lack of a clear scientific definition and standard measurement, and the lack of full consideration of social factors (Dunn Cavelty et al., 2023; Smith, 2023). Despite this, there are a few basic ideas that serve as a roadmap in the world of cyber threats.

2.2 Cyber Resilience in the Context of Education

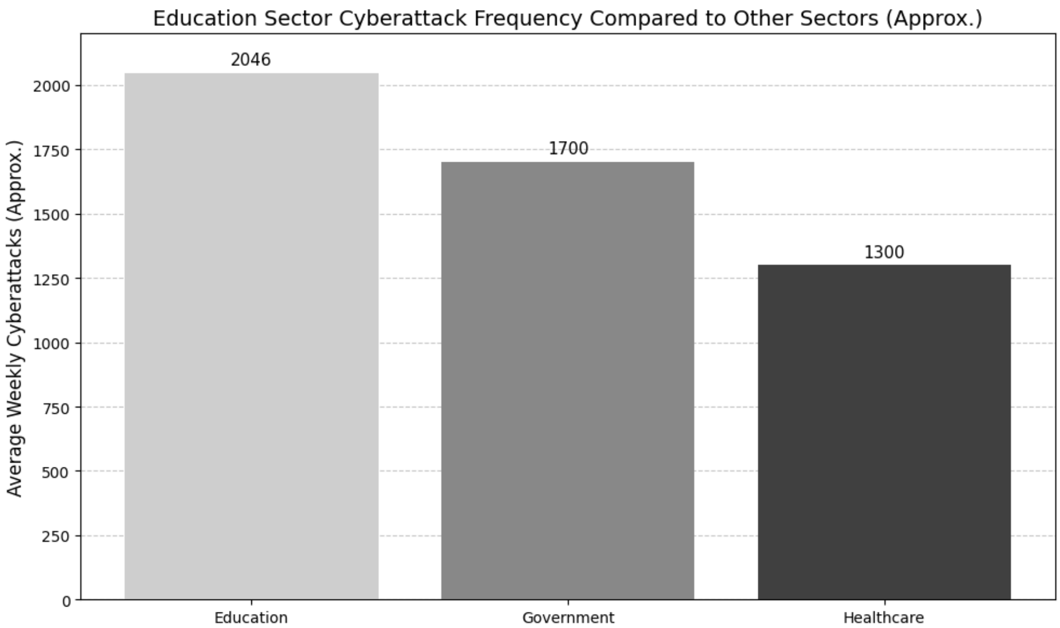
Large amounts of sensitive data, such as student and staff records, research, and financial data, are processed by educational institutions. In addition, increasing reliance on digital technology for teaching, learning, administration, and communication, educational institutions such as K-12 schools and colleges present a wealth of chances for cyberattacks. However, they typically have fewer resources and cybersecurity expertise than commercial companies, making them a simpler choice. Therefore, even though the materials prepared in terms of cyber resilience do not particularly address models for education, the situation of education institutes and concepts is very applicable.

According to the NIST CSF, cyber resilience is the ability to maintain administration and instruction in the face of cyberattacks such as ransomware, data breaches, or denial-of-service attacks on learning systems. Cyber resilience involves more than just technical safeguards for networks and data. Moreover, according to NIST, there are four features used to characterize cyber resilience. The first one is Anticipate/Prepare, which is about conducting risk analysis and creating protocols for communication and reaction. Also, it is about identifying specific hazards. For example, ransomware for administrative networks, phishing of staff/students, etc. Another feature is withstand/absorb, which allows the system to put measures in place to lessen the impact of an attack. For example, network segmentation, frequent backups, and strong authentication can be given. Thus, vital operations, such as restricted communication and crisis information access, can continue to run even in the event of an attack. To continue with the third feature, we have recovered. This is about restoring compromised systems and data as quickly as possible. The users should be able to save from backup, resume regular administrative and instructional practices, and deal with the fallout from the data breach. At the end, the cyber resilience of NIST CSF has been adapted. It is about growing teachers' awareness with training, modifying technology and procedures, and acquiring skills to learn from incidents. Therefore, developing a process or system design is intrinsically more resilient based on the lessons learned (Linkov & Kott, 2018; Alshar'e, 2023; Tzavara & Vassiliadis, 2024).

According to Bıçakcı and Evren (2025), it is primarily dependent on the awareness, readiness, and actions of students, teachers, administrators, and staff. In this context, fostering a positive cybersecurity culture through education and awareness-raising is therefore a crucial component of cyber-resilience (Al-Hawamleh, 2024).

2.2.1 Cyber Threats and Security in the Education Sector

According to Figure 2.2, there are many sectors are facing cyber-attacks especially education sector when it is compared to others(Checkpoint, 2024; Verizon Business, 2023). Digitalization has had a significant impact on the schools, and the COVID-19 pandemic has greatly accelerated this change (Fouad, 2021; Mouwers-Singh & Musikavanhu, 2024; Jawaid, 2023). K-12 institutions and other Higher Education Institutions (HEIs) need serious assistance and facilities in research, organizational management, and teaching; therefore, they are becoming dependent on digital solutions, cloud computing, distance learning environments, and network systems (Shelim, 2024; Jawaid, 2023). Although this digitalization has many benefits, it also exposes the education sector to an increasing number of different cyber threats (Ulven & Wangen, 2021). The education sector has weaker security systems compared to the financial or medical sectors. Additionally, due to the wealth of valuable information stored, educational institutions can be targeted by hacker groups (Fouad, 2021; Ulven & Wangen, 2021; Jawaid, 2023). Statistics show that ransomware and phishing are among the most common cyber threats affecting educational institutions worldwide; unfortunately, there is a significant increase in these threats (Jawaid, 2023; Fouad, 2021). In order to effectively mitigate these threats, it is imperative to be thoroughly aware of the potential attacks facing the education sector.



(Check Point, 2024; Verizon Business, 2023)

Figure 2.2 Education Sector Cyberattack Frequency Compared to Other Sectors

2.2.2 Cybersecurity Challenges in Educational Institutions

There are unique vulnerabilities to education sectors' security that differ from those facing most other businesses (Ulven & Wangen, 2021; Fouad, 2021). First, for a longtime financial consideration has been a major obstacle that educational institutions have struggled with minimal cybersecurity budgets; because of that, research showed that there is a shortage of qualified IT security experts and instructors who can offer suitable defense and training (Ulven & Wangen, 2021; Shelim, 2024; Fouad, 2021). The traditional academic culture of transparency and collaboration also exists in these institutions, and this culture sometimes opposes applying strict security measures to information sources (Ulven & Wangen, 2021; Fouad, 2021). Also, large, diverse, and transient user groups such as students, staff, faculty, researchers, and visitors, cause exposure because of the complex working conditions in the sector. In other words, having widespread BYOD policies, decentralized IT administration, and a combination of new and legacy systems makes the system easier to expose (Fouad, 2021; Ulven & Wangen, 2021; Jawaid, 2023). Furthermore, research indicates that teachers and students are not adequately trained in cybersecurity and are not sufficiently sensitized, making them vulnerable to phishing and social engineering attacks (Mouwers-Singh & Musikavanhu, 2024; Sağlam, Miller, & Franqueira, 2023; Ulven & Wangen, 2021). Thus, these institutions must stay up to date with a constantly changing threat landscape, which includes more complex attacks, and the need to safeguard newly implemented technology for research and teaching purposes (Fouad, 2021; Mouwers-Singh & Musikavanhu, 2024).

2.2.3 The Importance of Protecting Educational Data

Cybersecurity is vital for educational institutions because it protects sensitive and complex data (Ulven & Wangen, 2021; Shelim, 2024). For example, information of staff, prospective staff, alumni, students, and prospective students is protected. This is usually personally identifiable information (PII) such as names, addresses, social security numbers, and contact information; accordingly, much of the data that needs to be protected in schools is included in this and administrative data (Ulven & Wangen, 2021; Fouad, 2021). Moreover, educational institutions process sensitive data, such as financial data, including payroll, tuition, and donor information. Health data from student clinics and valuable intellectual property from research projects are also present in schools (Shelim, 2024; Ulven and Wangen, 2021; Fouad, 2021). Data breaches and individual identity theft can lead to catastrophic consequences, such as having to pay a ransom to recover employee data and severe financial losses. Therefore, this will damage the reputation of an institution, disrupt research and core academic functions, and lead to potential legal action against the school under information security laws (Mouwers-Singh & Musikavanhu, 2024; Fouad, 2021; Ulven & Wangen, 2021).

2.2.4 The Cyber Resilience Status of Teachers

Cyber resilience capabilities go beyond general cybersecurity to include specific knowledge, skills, and attitudes required to use the digital environment securely and resiliently (Korukluoğlu, Alcı, & Rubach, 2023; Santhosh & Thiyagu, 2024). These competencies include technical components such as password management and software updates, as well as cognitive components such as threat identification and critical information assessment; in addition, they include practical components such as spontaneous incident management, debriefing, and deployment of secure applications (Guillén-Gámez, Martínez-García, Alastor, & Tomczyk, 2024). Furthermore, the NIST Cybersecurity Framework is an example of a tool that organizes these complex competencies. Gaps in digital literacy among educators related to cybersecurity have been frequently documented in the literature. Several studies have examined specific areas of digital competence. Despite emphasizing basic protective skills, they found a severe lack of threat detection, incident response, and system or data recovery after an incident. This suggests an imbalance between proactive or reactive attitudes and basic protective skills. Another study on pre-service teachers reveals a general lack of preparation (Santhosh & Thiyagu, 2024) and weak digital security competencies (Guillén-Gámez et al., 2024).

The increasing use of digital technology in classrooms has changed how teachers and students learn and teach. However, it has made schools and their teachers more vulnerable to various cyber threats (Kuş & Mert, 2024). Schools are increasingly exposed to phishing and ransomware attacks and lack the necessary security capabilities despite hosting sensitive data (Ravichandran, Singh, & Sasikala, 2025). In addition, research by Wohlfart & Wagner (2023) suggests that teachers' cyber resilience level is often insufficient to meet the demands of the modern digital world. It is vital for educators to acquire the degree of cyber resilience they exhibit, that is, the ability to anticipate, prevent, absorb, and recover from malicious cyberattacks (Wohlfart & Wagner, 2023). Teachers need to adapt to the modern digital world and be aware of online dangers; they should also have cybersecurity and resilience awareness (Wohlfart & Wagner, 2023). This situation shows that education systems worldwide need support, training, and policy development (Ravichandran et al., 2025; Wohlfart & Wagner, 2023).

Due to the development of digital technologies, primary school teachers now need to teach using technology in addition to traditional education (Ayyildiz, Yilmaz, & Baltaci, 2021; Fitria & Suminah, 2020). In this context, teachers are now expected to serve both as teachers who use technology and as technology guides for students. In addition, they need to take on the role of digital change agents and help students navigate the increasingly complex digital environment safely (Fitria & Suminah, 2020). In this case, they need to raise their students as ideal digital citizens, which includes using digital systems safely, responsibly, and ethically; therefore, they need to integrate digital technology into the classroom (Kuş & Mert, 2024; Ayyildiz et al., 2021). In addition, educators manage student and school data; therefore, they play a significant role in protecting data security and privacy in the school environment (Ravichandran et al., 2025). Primary school teachers are the first to defend against cyber threats in the classroom; in addition, they are responsible for teaching their students how to avoid potential dangers such as phishing and cyberbullying (Sezer, 2015). In this case, educators must continuously develop their skills and knowledge while practicing cyber resilient behaviors (Fitria & Suminah, 2020; Santhosh & Thiyagu, 2024). As a result, in today's digital education environment, no teacher role does not include cybersecurity and resilience responsibilities that rely on more than just technical expertise; however, it still requires a clear interest in digital security for both students and the instructor.

According to Ravichandran et al. (2025), the foundation of teachers' cyber resilience is their understanding of cybersecurity. Studies show that educators often express a lack of confidence in their cybersecurity and digital literacy skills (Altinöz et al., 2019). Also, this is often supported by reports of teachers' lack of formal cybersecurity training (Ravichandran et al., 2025). Ravichandran et al. (2025) also note that awareness of threats is uneven among primary school teachers in India, with most having basic knowledge of threats such as identity theft or phishing; however, they found that very few teachers knew of threats such as DoS attacks or digital theft. In addition, this study found that teachers often underreport cyber incidents. In addition, they were not aware of complaint channels when such incidents occurred. They relied more on social media and newspaper reports rather than official cybersecurity education channels. On the other hand, while some dangers, such as cyberbullying, are well understood (Sezer, 2015), there is evidence that teachers' understanding of cybersecurity is often unstable, inadequate, and not well supported by institutional structures and educational programs (Ravichandran et al., 2025; Santhosh & Thiyagu, 2024). The frequency of Internet use and gender may influence knowledge levels, but the bottom line is that there is a continuing need to develop knowledge across all cyber resilience capabilities.

2.3 Cybersecurity Frameworks and Standards

This chapter highlights some frameworks and standards businesses use to manage cybersecurity risk. The frameworks provide formal approaches for improving cybersecurity, reducing risk, and cultivating resilience to attacks. What is particularly relevant to sectors with unique issues and sensitivities, such as education, is how to utilize and adapt. Large frameworks like ISO 27001, COBIT, and the NIST Cybersecurity Framework provide a variety of governance, risk management, and compliance options.

2.3.1 An Overview of Prominent Cybersecurity Frameworks

The landscape of cybersecurity employs various frameworks designed to guide organizations in managing their cybersecurity risks and establishing effective governance. Among the widely adopted frameworks are ISO/IEC 27001, COBIT, and the NIST Cybersecurity Framework (CSF), each offering a structured approach to address diverse organizational needs and objectives (Alwahaibi et al., 2022; Taherdoost, 2022).

ISO/IEC 27001 is an international standard developed by ISO and IEC. It aims to establish, implement, maintain, and continuously improve the Information Security Management System (ISMS) (ISO, 2013; Taherdoost, 2022). In addition, a systematic approach to risk assessment and solutions is required to achieve certification (Alshar'e, 2023; Alwahaibi et al., 2022). It is a framework built on the Plan-Do-Check-Act cycle; It also includes a list of control objectives and measures (Taherdoost, 2022). In other words, it is a prescriptive and risk-based standard, so it requires documentation and checklists based on identified risks (Alshar'e, 2023; ISO, 2013). The formal certification of ISO 27001 is often a key factor for stakeholders (Alshar'e, 2023; Alwahaibi et al., 2022). In short, it is essential for any organization that wants to implement and certify an ISMS, especially those with a global presence or operating in highly regulated sectors (Alwahaibi et al., 2022).

COBIT, developed by ISACA, serves as a comprehensive framework for the governance and management of enterprise IT (Taherdoost, 2022). This framework is IT-centric and aims to align IT with business objectives. It prioritizes creating value, optimizing risk and resources, and ensuring security in a governance context. COBIT is based on processes, control objectives, principles, and enablers when determining governance and direction objectives (Taherdoost, 2022). Thanks to its process-oriented structure, it details the management and control of IT assets; thus, it enables organizations to meet business objectives while considering risk and security in the IT governance environment (Alwahaibi et al., 2022). Unlike ISO 27001, COBIT does not directly offer corporate certification. However, it is aimed at organizations looking to improve their enterprise IT governance and management; in addition, this framework provides a solid framework to facilitate alignment between IT and business strategies and improve communication with stakeholders (Alwahaibi et al., 2022).

The NIST Cybersecurity Framework (CSF), developed by the U.S. National Institute of Standards and Technology, offers a voluntary framework initially designed for critical infrastructure but now widely adopted across various industries (NIST, 2018). Its primary focus is on managing cybersecurity risk, improving cyber resilience, and facilitating risk communication among stakeholders, emphasizing outcomes over strict controls (NIST, 2018; Taherdoost, 2022). The CSF comprises three key components: the Core, Implementation Tiers, and Profiles. The Core is further organized into five fundamental Functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2018). While NIST CSF 2.0 introduces a "Govern" function, the initial research scope focused on the original five functions. The NIST CSF is characterized by its risk-focused, outcome-oriented, flexible, and dynamic nature, allowing for voluntary alignment with existing standards and practices like ISO 27001 and COBIT (Alshar'e, 2023; NIST, 2018). Implementation is typically assessed through self-evaluation or third-party audits, as no formal certification exists (Alshar'e, 2023). Its adaptability through Profiles enables organizations to tailor their application to their specific risks, priorities, and objectives (NIST, 2018). Originally intended for U.S. critical infrastructure, the NIST CSF is now utilized by organizations of all sizes and sectors, including education, to develop or enhance their cybersecurity risk management programs (Alwahaibi et al., 2022; NIST, 2024).

In essence, ISO/IEC 27001 provides a framework for establishing a certified ISMS, COBIT focuses on the governance and management of enterprise IT, and the NIST CSF offers a flexible approach to managing cybersecurity risk and enhancing resilience. Each framework contributes uniquely to the broader cybersecurity landscape, catering to different organizational priorities and maturity levels.

2.3.2 Adaptation of Cybersecurity Frameworks to the Education Sector

HEIs and K-12 education sectors have unique cybersecurity demands and difficulties. This includes dealing with massive amounts of personal data for students and employees under laws such as FERPA (The Family Educational Rights and Privacy Act) in the United States. There is often a need to serve many different technical levels to end users in terms of cyber security; unfortunately, limited security, staffing, and IT budgets should be considered as well. On the other hand, for educational places open networking structures must be implemented to facilitate academic freedom, research, and teamwork (Shelim, 2024; Taherdoost, 2022). Therefore, standard cybersecurity models need to be modified to fit this context. As is known, schools are an appealing target for ransomware, phishing, and data breaches since they hold private personal information. For example: health records, student records, financial records, staff information, academic research data (Alwahaibi et al., 2022; Ronen, 2024). Cyber security system must secure these assets without unduly interfering with the research and academic objectives. Security awareness must be increased with security training for staff members, teachers, and students; in spite of that, facilities and personnel to provide comprehensive security measures are often restricted (Shelim, 2024). On the other hand, because of its inherent adaptability, flexibility, and risk-based way of thinking, The NIST CSF is particularly well-suited for adaptation in the education business when it is compared to ISO27001 and COBIT (NIST, 2024; Taherdoost, 2022).

ISO 27001 is appropriate for large businesses that require a full, certified ISMS, but it is prohibitively expensive and difficult to implement (Alshar'e, 2023; Alwahaibi et al., 2022). COBIT effectively improves IT governance and institutional goal alignment in high-complexity university contexts, but it is less focused on day-to-day operational cybersecurity than NIST CSF (Alwahaibi et al., 2022).

On the other hand, NIST CSF provides flexibility based on profiles. In other words, educational institutions can develop custom "Profiles" based on their specific risks. For example, Profiles can be created based on K-12 student or university research data, budget, regulatory constraints, and priorities. This provides a security plan suited to each institution's unique situation (NIST, 2018). Moreover, NIST CSF directs institutions to allocate limited resources to secure vital assets. For example, student information systems, research databases, and protecting against threats, such as phishing attempts against staff and students. (NIST, 2018). Furthermore, in CSF 2.0, The Core Functions cover the entire security lifecycle relevant to education, including identifying key assets, implementing protections such as access controls. It also includes awareness training, detecting unusual behavior, responding to incident response plans, and data backup and recovery (NIST, 2018). These functions establish a framework for assessing and enhancing teacher cyber resilience. Moreover, thanks to its easy and common language, architecture allows easy information sharing regarding cyberattacks and obligations among various stakeholders in an academic environment (NIST, 2018). Also, the structure of NIST CSF can be used to create cybersecurity awareness courses and employee/student training modules focused on desired security outcomes (Shelim, 2024; NIST, 2018).

2.3.3 Reasons for Choosing the NIST Cybersecurity Framework

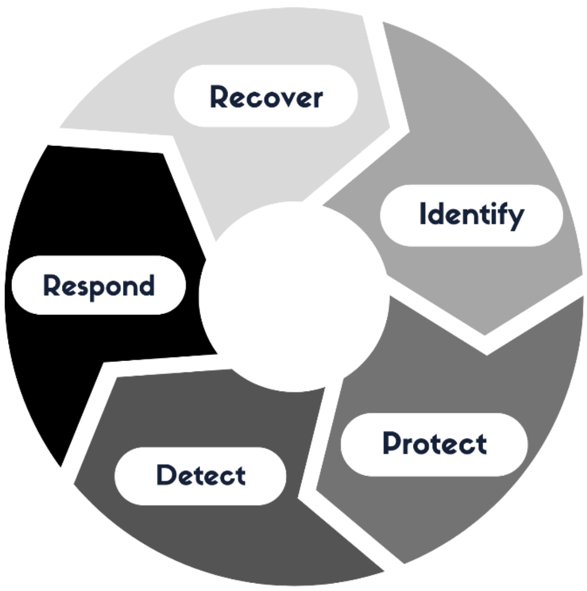
Unlike strict rules, the NIST CSF concerns desired security goals rather than specific procedures. Due to its goal-oriented versatility can be applied to different school environments, diverse technical infrastructures, and varying levels of digital literacy among educators. It is necessary to measure a capability such as cyber resilience. Adaptability is also critical to measuring a concept that includes technical controls within an institution (Taherdoost, 2022). The NIST CSF promotes risk awareness and prioritization, considering the environment in which it is located. For educators, this is to help them become aware of the hazards associated with the materials they teach and the cyberattacks they are exposed to. This is directly related to the assessment of resilience, which requires risk awareness. As it shown in the Figure 2.3, the NIST CSF has five core functions to provide the core competencies of cyber resilience in the environment in which it is located (NIST, 2018). These functions are necessary to determine how cyber resilience will be measured in the system. In other words, the

NIST CSF creates a standard vocabulary for describing cybersecurity capabilities and outcomes. For example, it allows us to measure how much it prevents and how teachers identify threats, respond to attacks, and facilitate recovery processes. Therefore, this framework allows us to measure teachers' behaviors at various stages and practices. It is also open to using scenario- or simulation-based techniques, such as your research. This CSF allows researchers, educators, school administrators, and IT professionals to examine cybersecurity expectations and outcomes. It facilitates presenting your cybersecurity analysis results to relevant stakeholders (Taherdoost, 2022). In addition, since the framework focuses on desired outcomes or endpoints, it is more understandable for non-technical stakeholders, such as teachers (NIST, 2018). This way, all employees understand the security goals without needing technical background knowledge. Therefore, it makes it suitable for administrators and IT teams to assess teachers' awareness and behavioral responses. Although the NIST CSF was initially designed for use with critical infrastructure, it is now widely used in many sectors, including education in the United States (Alwahaibi et al., 2022; NIST, 2024; Taherdoost, 2022). Its use in higher education for risk management documents and curriculum documents demonstrates its applicability; thus, it can be extended to the K-12 educational context (NIST, 2024). Additionally, unlike ISO 27001, the NIST CSF is entirely voluntary and free, meaning no formal certification mechanism (Alshar'e, 2023). This makes the NIST CSF more attractive and accessible to resource-poor educational institutions. Therefore, NIST CSF is the best alternative to align cybersecurity measures with the education sector due to its flexibility, adaptability, and risk-based character. Because it can address complex and demanding needs, ranging from the lack of cybersecurity infrastructure in the education sector to the lack of training and awareness in the sector.

2.4 NIST Cybersecurity Framework

As mentioned above, NIST CSF is an excellent and extensively used tool to reduce and manage cybersecurity risks for organizations (Cybersecurity and Infrastructure Security Agency [CISA], 2020; Gordon, Loeb & Zhou, 2020; NIST, 2018;

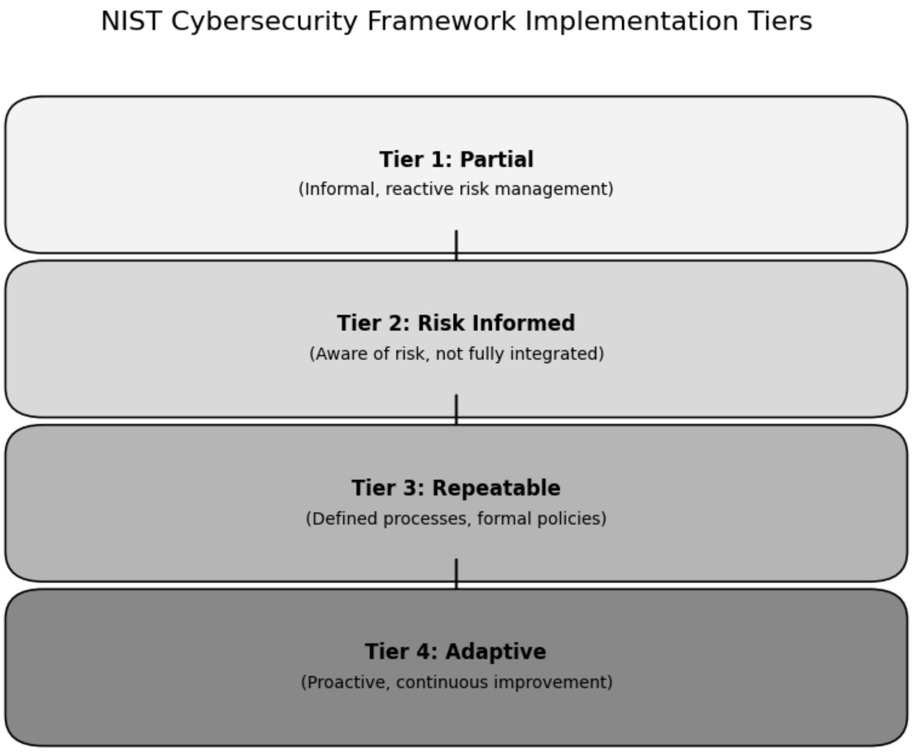
Organization of American States [OAS] & Amazon Web Services [AWS], 2019). Since it is flexible, voluntary, and risk-based, it has been widely implemented across industries, sizes, and regions. It was created to enhance the cybersecurity of the United States' critical infrastructure (NIST, 2018; Taherdoost, 2022; White & Sjelin, 2022). The CSF has a standard and basic language; also, it offers a structured approach to help businesses define, quantify, prioritize, and share their cybersecurity efforts (Khan, 2023; NIST, 2024). The CSF has three parts, and the first one is the framework core. This part is about using Functions, Categories, and Subcategories to define desired outcomes. The second core of NIST CSF is Implementation Tiers. This is about specifying how serious an organization's risk is while handling practices. The last core is Framework Profiles, which connect cybersecurity activities to organizational goals and needs (NIST, 2024; White & Sjelin, 2022). The main goal of the Framework is to enhance, not replace, current cybersecurity efforts and risk management strategies (NIST, 2018; Taherdoost, 2022).



(NIST, 2018)

Figure 2.3 NIST Cybersecurity Framework

The NIST CSF Tiers establish the organization's degree of cybersecurity risk management and governance. It establishes the general tone for how cybersecurity risk will be managed and outlines how the organization views the risk and how it will be addressed through organizational procedures. As it shown in the Figure 2.4, the tiers start at Tier 1, which is Partial. Moreover, it consists of reactive and temporary measures, procedures, and awareness, which are limited. Then it continues with agile practices on a path of continuous improvement. There is a progression to Tier 4, Adaptive, where practices are adapted based on timely intelligence, predictive indicators, and lessons learned. Since the application of CSF Functions is carried out temporarily, it is based on established practices. Based on the threat landscape and company goals, it can be repeatable, policy-driven, adaptive, and dynamically changing. The selected Tier determines the level of maturity and integration expected across the company's entire cybersecurity initiative.



(NIST, 2018)

Figure 2.4 NIST Cybersecurity Framework Implementation Tiers

2.4.1 Historical Development and Purpose of the NIST Framework

The NIST Cybersecurity Framework emerged in the context of concerns about infrastructure that is essential to both national security and the economic security of the United States (Executive Order 13636, 2013; Office of the Federal Register [Federal Register] , 2013). In response to the growing concerns in February 2013, the Executive Order titled "Improving Critical Infrastructure Cybersecurity" was signed. NIST was then tasked with overseeing the creation of a voluntary framework to reduce cybersecurity risk (Executive Order 13636, 2013; NIST, 2013). The goal was to create a flexible, repeatable, performance-based, and cost-effective framework based on cybersecurity using best practices and current standards (Executive Order 13636, 2013, Section 7b; Gordon et al., 2020). As such, they engaged in a significant participatory process based on Requests for Information (RFI), public workshops, and review windows; In addition, work began with governments, businesses, academics, and extensive stakeholder participation (Federal Register, 2013; NIST, 2013; White & Sjelin, 2022). The diverse work process allowed for adaptation to real-world needs and practices.

CSF 1.0 was published in February 2014; then, it was updated in April 2018 with more additions and features. In other words, it was republished with improvements in the areas of self-assessment, supply chain risk management, and identity verification (NIST, 2018; Taherdoost, 2022). In February 2024, CSF 2.0 was published, placing even more emphasis on governance and expanding its applicability scope (NIST, 2021; NIST, 2024). Despite this, the framework's core goal has remained constant throughout its development: simply providing a simple language and structure to effectively and responsively manage cybersecurity risk across a variety of organizational contexts (Gordon et al., 2020; NIST, 2024). Therefore, Table 2.1 shows the changes between the NIST CSF models over the years.

Table 2.1 NIST CSF Descriptions Over the Years

Step / Concept	**Nist Csf 1.0 Description**	**Nist Csf 1.1 Description**	**Nist Csf 2.0 Enhancement/description**
1. Scope and Prioritize	Basic infra, sizing.	Formal phase, setting priorities.	Governance integration, link strategy/risk/and compliance.
2. Mapping and Orientation	Context, assets, threats.	Formal step, SCRM focus.	Governance stakeholders, quantitative risk (optional).
3. Create Current Profile	Current State concept.	Standard assessment, baseline.	Dynamic profile, real-time data, continuous monitoring.
4. Conduct Risk Assessment	Fundamental activity.	Distinct phase, includes SCRM.	Emphasis on quantitative, governance engagement.
5. Create Target Profile	Target State concept.	Formal phase, feasible ideal state.	Governance and continuous improvement integration.
6. GAPS: Identify, Analyze, Prioritize	Risk-based prioritization logic.	Separate step, impact/resource prioritization.	Detailed risk-based prioritization, linked to Governance, and continuous analysis.
7. Adopt an Action Plan	Using gaps, refinement.	Codified, written plan, high-risk priority.	Governance, monitoring, tracking, revision.
8. Govern (New CSF 2.0 Function)	Not separate.	Not separate.	New core function, determining/overseeing plan/roles/general governance, integration.

Table 2.1 demonstrates the changes in NIST CSF over the years: NIST CSF 1.0 from 2013, 1.1 from 2018, and 2.0 from 2024 compared to scope and prioritizing, mapping and orientation, creating current profile, conducting risk assessment, creating target profile, GAPS, identifying, analyzing, and prioritizing, adopting an action plan, and new governance function.

2.4.2 Identify Function

NIST's Cybersecurity Framework relies on Identify to generate the organizational knowledge needed to manage cybersecurity risk (Khan, 2023; NIST, 2024; Taherdoost, 2022). The context of this function includes knowledge about the relevant cybersecurity risk and the resources available for attack for critical functions (NIST, 2018; OAS & AWS, 2019). Resource management is the core activity under this function; moreover, it includes cataloging physical devices, systems, software platforms, and data according to their importance to the organization and investigating their potential for attack (Federal Trade Commission [FTC] 2016; Khan, 2023; NIST, 2024). Examples of this function include conducting risk assessments to identify threats, vulnerabilities, and their potential harms for cybersecurity risk; and establishing governance arrangements (Khan, 2023; NIST, 2018). Developing a risk management strategy, such as risk tolerance (NIST, 2018) and improving cybersecurity supply chain risk management are the functions of this function (NIST, 2024). Therefore, by applying these activities, organizations can focus more specifically on cyberattacks, allocate resources wisely, and customize cybersecurity efforts to achieve their goals (CISA, 2020; NIST, 2018; White & Sjelin, 2022).

2.4.3 Protect Function

The Protection function requires the establishment and implementation of appropriate preventive measures, thus helping to reduce the impact of potential cybersecurity incidents and maintain essential activities (Khan, 2023; NIST, 2024). After the risk is identified, i.e., the Identification function and the determination of priorities, the

Protection function includes the implementation of asset protection measures to maintain operational resilience (NIST, 2018; OAS & AWS, 2019). Identity management, authentication, and access control are important activities of the Protection function. These include limiting access to authorized personnel, processes, or devices (NIST, 2024; Taherdoost, 2022). It also includes training teachers and employees; thus, increasing their awareness (Khan, 2023; NIST, 2018). In addition, it is necessary to ensure confidentiality, integrity, and availability in this function; therefore, it is necessary to implement data security measures in institutions (FTC, 2016; NIST, 2024). This function includes information protection processes such as configurations, backups, and data destruction, and it also includes technical activities such as the implementation of procedures and system maintenance (NIST, 2018). In addition, the use of measures such as network segmentation or malware defense is also among the duties of the protection function (NIST, 2018; White & Sjelin, 2022). It has been stated in the updates of NIST CSF that Technology Infrastructure Resilience is also important (NIST, 2024). In short, the protection function is essential to reduce the impact of cybersecurity breaches before they occur (CISA, 2020; OAS & AWS, 2019).

2.4.4 Detect Function

The detection function's purpose is to create and implement necessary actions to detect a cyber threat when it occurs (OAS & AWS, 2019; NIST, 2024). This function allows companies to quickly detect attacks or other unwanted events, allowing them to fix defensive controls and recover operations (NIST, 2018; Taherdoost, 2022). There are basic activities to detect cyberattacks. Some of these are, for example, observing events and anomalies by looking at data from the network, physical environments, personnel usage, and external sources (FTC, 2016; NIST, 2024; White & Sjelin, 2022). There is also the implementation of Security Continuous Monitoring procedures to stay informed about the cybersecurity situation and detect changes (NIST, 2018). Additionally, the mission of this function is to define Detection Procedures that include role identification, compliance assurance, process testing, and incident information communication (NIST, 2018; Taherdoost, 2022). It relies on correlation from multiple sources of information and basic network activity information to successfully detect changes that may indicate an attack or compromise (CISA, 2020; NIST, 2024).

2.4.5 Respond Function

In this function, the goal is to plan and execute appropriate actions to address a problem as soon as it is discovered (NIST, 2024; Khan, 2023). In other words, to effectively and efficiently prevent a real or suspected cybersecurity attack (OAS & AWS, 2019; NIST, 2018). Response Planning, which involves creating a plan and implementing it as soon as an incident is detected, is performed (Taherdoost, 2022; NIST, 2018). For example, it includes managing communication with internal and external stakeholders, including coordinating interventions and reporting incidents when necessary, during the resolution process (NIST, 2024). It is similar to conducting analysis to determine the nature, scope, and root cause of an incident, which usually involves forensic science (Khan, 2023; NIST, 2018). In other words, the activities of this function are performed to prevent the incident from becoming more widespread and to eliminate it (NIST, 2018; White and Sjelin, 2022). Additionally, remediation is accomplished by using lessons and experiences learned from the response to improve future planning (NIST, 2018). A successful response function reduces incident costs, reputational damage, and disruptions to operations (CISA, 2020; FTC, 2016).

2.4.6 Recover Function

The main objectives of the recovery function are to restore all operations or services that are compromised due to a cybersecurity incident; also, to maintain resilience plans by completing the necessary steps (Khan, 2023; NIST, 2024; OAS & AWS, 2019). In other words, this function facilitates a rapid return to normal operations by minimizing the overall impact from the incident (NIST, 2018; White & Sjelin, 2022). According to the FTC (2016) and NIST (2024), recovery planning is to develop and maintain procedures to recover systems and assets. It is also to increase ultimate resilience with lessons learned from previous incidents. It is the duty of this function to incorporate experiences into recovery tactics and coordinate activities. In addition, communicating with internal and external stakeholders to manage expectations is also a basic recovery activity. Organizational resilience, which enables businesses to respond to and quickly recover from devastating cybersecurity attacks, depends heavily on successful recovery planning (CISA, 2020; Khan, 2023).

2.5 Teachers' Cyber Resilience and Factors Influencing

The increasing global digitalization of education requires addressing teachers' positions regarding cybersecurity awareness and cyber resilience. Teachers are also responsible for protecting sensitive data and encouraging students to use the Internet consciously (Nugroho et al., 2024). In addition, research in this field reveals similar problems and context-dependent differences in Türkiye and various international areas. By comparing these findings, it is possible to determine context-dependent and general criteria for establishing teachers' cyber resilience.

2.5.1 Understanding Teacher Cyber Resilience and Awareness

The increasing use of digital tools in education has made cybersecurity a vital priority for teachers (Amoroso & Magnan, 2025). This situation brings with it the responsibility for teachers to protect sensitive information and ensure the safety of students in virtual environments (Amoroso & Magnan, 2025). Turkish academic sources state that teachers produce and store information in digital environments and that the security of this digital data is fundamental (Çetinkaya, Güldüren & Keser, 2017). Therefore, educational institutions and teachers are attractive targets for cyberattacks due to housing large amounts of sensitive data belonging to students, staff, and faculty (Readiness and Emergency Management for Schools, 2024; Amoroso & Magnan, 2025). This data includes Personally Identifiable Information (PII), students' academic records, health information, and teachers' personal and financial data (Readiness and Emergency Management for Schools [REMS], 2024; Student Privacy, 2024; Amoroso & Magnan, 2025). According to Linkov et al. (2013)

and NIST CSF, cyber resilience is an independent concept emphasizing foresight, survival, recovery, and adaptation.

2.5.2 Awareness Levels of Teachers

Studies conducted in Türkiye show that interest in classroom cybersecurity issues is increasing. A study conducted by Canoğulları (2021) found that teachers generally have a moderate level of awareness about information security and that teachers' cyber awareness was not at the desired level. The study by Varkan Kavas, Özbudak, and Çetkin (2022) also found moderate general awareness. Karagözlü (2020) looked at the behaviors of intern teachers to measure cybersecurity awareness and found that they used the internet unconsciously and without cyber resilience. According to previous studies, most Turkish educators believe that they do not have sufficient cybersecurity and digital literacy skills (Altınöz et al., 2019). Studies conducted in Türkiye align with international reports on the general inadequacy of cybersecurity preparedness.

Furthermore, there are deficiencies, especially in detecting threats such as phishing or understanding more complex security concepts (Varkan Kavas et al., 2022; Eroğlu, 2023). Studies have shown that 60% of teachers are inadequate in detecting phishing emails (Eroğlu, 2023). Canoğulları's (2021) study found that teachers are aware of online scams and frauds; on the other hand, it emphasized that teachers are unaware of other threats, such as malware and social engineering/phishing. This study showed moderate awareness, especially in the "Attacks and Threats" sub-dimension (Canoğulları, 2021). Studies show that teachers have lower awareness of lesser-known topics such as firewalls, security certificates, or secure online storage (Varkan Kavas et al., 2022). An article by Ravichandran et al. (2025) found that 75% of teachers are aware of phishing. Tomczyk's (2024) study indicates that some teachers can detect cyberattacks by monitoring the internet or through reporting by third parties, while some attempt to identify the source themselves. However, the inability to always find the perpetrator or the anonymity of the attack shows that detection ability varies and is not always successful (Tomczyk, 2024). A study by Ravichandran et al. (2025)

revealed that 60% of teachers were unaware of existing reporting mechanisms for reporting cybersecurity concerns.

2.5.3 Observed Security Practices and Preparedness Indicators

A study conducted with 870 teachers in Balıkesir revealed that 78% of teachers store students' Turkish ID numbers in unencrypted environments (Yılmaz et al., 2016). Research indicates that practices such as not using strong passwords and sharing passwords with unauthorized individuals threaten digital data security in school administration (Aslanlı & Özdoğru, 2023). Studies indicate that practices such as not using secure passwords threaten digital data security in school administration (Kruger, Drevin, & Steyn., 2010). However, research has also found that teachers are highly aware of creating secure passwords (Yılmaz et al., 2016). Previous studies show that antivirus program usage rates were low (Yıldırım & Varol, 2013; Kaşıkcı, Çağıltay, Karakuş, Kurşun, & Ogan, 2014); on the other hand, new studies have revealed that teachers are knowledgeable about using antivirus software and the usage rate is high (81.5%) (Kapanoğlu, 2016; Canoğulları, 2021). Therefore, it is stated that teachers' awareness of the importance of using antivirus software is high (Çetinkaya, Güldüren & Keser, 2021). The Protect function of the NIST Cybersecurity Framework involves implementing necessary safeguards. Research indicates that while basic cybersecurity measures (antivirus software, security firewalls) are widely implemented, more advanced solutions like multi-factor authentication and data encryption are less adopted (Anwar, Juanda, Anderson, & Williams, 2024).

Moreover, outdated software can contain vulnerabilities that cyber attackers can exploit; according to a study by IKON Insights (2024), 43% of cyberattacks originate from vulnerabilities in outdated software. Ravichandran et al. (2025) state that teachers need a more profound awareness regarding regular software updates. Multi-factor authentication (MFA) provides an additional layer of security and significantly reduces the risk of unauthorized access (Student Privacy, 2024; Center for Information Security Awareness [CFISA], 2023; CISA, 2024). It has been proven that using MFA reduces the risk of unauthorized access by 67% (IKON Insights, 2024). The response function of the NIST Cybersecurity Framework involves implementing activities in response to a detected cybersecurity event. Tomczyk's (2024) study identified significant variations in how teachers respond to cyberattacks. The Recover function of the NIST Cybersecurity Framework supports the implementation of plans for the timely restoration of activities impaired by a cybersecurity event.

2.5.4 Factors Influencing Teacher Cyber Resilience

This section examines, as in similar studies, demographic and behavioral factors such as gender, proficiency in digital tools, daily internet use, professional qualifications, and whether cybersecurity training affects teachers' cyber resilience levels, as well as related awareness and behaviors.

Gender

Regarding gender, the literature presents varied findings. A meta-analysis conducted in Türkiye found a negligible and statistically insignificant difference between the resilience levels of women and men (Arı & Çarkıt, 2020). Similarly, another study in Türkiye that analyzed teachers' experiences with cyberbullying found no significant differences between male and female teachers in terms of their involvement in cyberbullying, experiences of cyber victimization, or their overall cyber sensitivity (Çelik & Kaya, 2019). Conversely, research involving pre-service teachers in Türkiye revealed that male candidates demonstrated higher scores in digital fluency than female candidates (Kabataş Memiş, 2023). Sapanca and Kanbul (2022) found a gender disparity in awareness; moreover, they found that male pre-service teachers scored higher on awareness and knowledge scales. One study in Jordan also indicated that male teachers exhibited a higher level of cybersecurity awareness than their female counterparts (Al-Habashneh, 2023). The higher cybersecurity awareness among male teachers in Jordan contrasts with the lack of significant gender differences in cyberbullying-related variables and the negligible difference in general resilience observed in Türkiye. Research on refugees in Türkiye indicates that resilience can manifest differently between genders (Bawadi, Abu-Shanab, Al-Twalbeh, & Alomari, 2022; Yee, Mahmud, & Alias, 2020), suggesting that interventions aimed at fostering resilience might need to be gender-sensitive (Bavli & Kortel, 2023; Stuart, 2025). This indicates that gender differences are context-dependent or skill-dependent and that gender alone may not be the primary determinant of cyber resilience.

Digital Tool Competencies

Effective and efficient use of digital technologies can be considered a key element of digital tool competence (Özer, 2022); therefore, it may indirectly affect cyber resilience. Studies conducted in Türkiye also highlight significant gaps in teacher training and education. According to previous studies, most Turkish educators believe that they do not have sufficient cybersecurity and digital literacy skills (Altınöz et al., 2019). Noyan and Güleç (2024) observed the complex connection between the teaching-learning environment and emphasized that they must improve themselves to adapt to digitalization. Benzer and Karal (2023) found that teacher candidates in all departments generally had moderate awareness levels, but the awareness levels of pre-service IT teachers were significantly higher. It is important to acknowledge that teachers might not always be adequately prepared for the complexities of online teaching and the associated security risks (Bavli & Kortel, 2023; Adıgüzel, Kaya, & Ersoy, 2024).

Moreover, a study conducted in Türkiye assessed the digital competence of teachers and found that, while they generally operated at an "integrative" and "expert" level in their use of digital tools, they still encountered various problems and expressed a need for professional support (Adıgüzel et al., 2024). One study examined teachers' digital competencies and identified essential components such as teachers' ability to locate and critically evaluate online information, understanding their digital footprint, and the skills necessary to secure their data access (Tomczyk, Wójcik, & Swacha, 2024). Safe and responsible use of social networking sites (SNS), understanding browser and email security settings, and the ability to recognize and report suspicious online activity were also identified as vital components of cyber resilience (Tomczyk et al., 2024; Adıgüzel et al., 2024). Self-efficacy, the belief in one's ability to succeed in specific situations (Bandura, 1994), also plays a role in cyber resilience.

Daily Internet Use and Screen Time

Studies have also linked internet use frequency to awareness levels in Türkiye and internationally (Sezer, Yılmaz & Yılmaz, 2015; Ahmed et al., 2021). One study found that most participating teachers reported using the internet for 1 to 3 hours daily, while smaller proportions used it for longer durations (Özker, 2022). This indicates varying levels of daily screen time involving internet use. However, excessive or uncontrolled internet use can negatively affect well-being and potentially reduce an individual's focus and awareness (Gökmen, Gökmen, & Horzum , 2023; Satici, 2019). Research examining problematic internet use among parents in Türkiye found negative correlations between excessive internet use and both happiness and psychological resilience (Gökmen et al., 2023). Resilience was also not associated with years of daily internet use, indicating that exposure is not always equivalent to preparedness (Sapanca & Kanbul, 2022).

Professional Experience

Studies indicate a significant difference among older teachers regarding the relationship between age and cybersecurity awareness (Canoğulları, 2021). Awareness tends to be higher among younger teachers and decreases with age (Yayla, 2018). This trend may be attributed to older teachers' later introduction to technology and their established teaching practices, potentially leading to less familiarity with protecting digital information (Canoğulları, 2021). Supporting this, research suggests that competencies in information technologies decrease with age, with teachers having fewer service years showing higher average competencies (Durak & Seferoğlu, 2017) and newly graduated teachers having higher IT self-efficacy perceptions than senior teachers (Demirer & Sak, 2015). The higher scores among younger teachers might be explained by their early technology exposure, easier adaptation to the information society, and knowledge of digital citizenship (Canoğulları, 2021). In contrast to age-related findings, a study investigating whether teachers' digital data security awareness differed based on their professional experience found no statistically significant difference (Yılmaz et al., 2016). These findings indicate that digital data security awareness did not change significantly with the number of years spent teaching (Yılmaz et al., 2016).

Cybersecurity Training

Studies conducted in Türkiye highlight significant teacher training and education gaps, stating that more education and awareness are needed (Şenoğlu & Çoklar, 2024). According to previous studies, most Turkish educators believe that they do not have sufficient cybersecurity and digital literacy skills (Altınöz et al., 2019). Benzer and Karal (2023) found that the awareness levels of pre-service IT teachers who had training on the subject were significantly higher than those in other departments. Cybersecurity training and professional development programs are important in developing cybersecurity skills (Adıgüzel et al., 2024). The availability and quality of cybersecurity training for teachers vary worldwide, with many schools reporting very little training. Continuous training is critical in informing teachers about common threats such as phishing and social engineering (Student Privacy, 2024; REMS, 2024; Amoroso & Magnan, 2025; CFISA, 2023; CISA, 2024). Specific cybersecurity workshops for teachers provide knowledge on effectively recognizing and mitigating cyber threats (CFISA, 2023). Training covering topics such as recognizing phishing attempts, securing personal devices, and understanding the importance of strong passwords can help teachers create a safe online environment for students (CFISA, 2023). The beneficial effects of cybersecurity education in enhancing cyber resilience have been documented in various contexts (Al-Habashneh, 2023). Cybersecurity training programs are essential but are often underutilized, leading to a reactive rather than proactive approach to cyber threats (Qawasmeh, Al-Qahtani & Khan, 2024). Lack of training and resources limits teachers' ability to detect, respond to, and recover from cyberattacks (Anwar et al., 2024; Tomczyk, 2024). National and global studies jointly underline the need for more efficient, valuable, and continuous training. According to the literature, providing resources and support such as workshops, online training, and peer networks is necessary.

2.5.5 Comparative Analysis of Literature Findings on Research Questions

This section provides a comparative analysis of the research findings concerning the research questions after reviewing studies carried out in Türkiye and overseas. By combining the data on teachers' levels of cyber resilience and influencing factors from various contexts, this analysis attempts to find commonalities, distinctive features, and significant areas of divergence or convergence in the literature.

Shared Cybersecurity Landscape and Vulnerability

The literature reveals a global consensus on the increasing importance of cybersecurity for educators and highlights both shared expectations and challenges in cyber resilience. Studies conducted in Türkiye mirror concerns reflected worldwide regarding teachers' awareness and resilience to cybersecurity issues, which are exacerbated by the growing reliance on digital technologies in education and the rising frequency of cyberattacks targeting the sector (Ronen, 2024; Check Point, 2022; Verizon Business, 2023). The education sector is globally recognized as a high-risk target, facing weekly attack frequencies higher than many other sectors combined, with phishing, ransomware, and data breaches being primary concerns (Check Point, 2022; Sophos, 2024). This highlights the universal vulnerability faced by educational institutions and their staff.

Common Challenges in Teacher Awareness and Preparedness

A striking similarity across studies in Türkiye and other countries is the well-documented lack of sufficient cyber knowledge and skills among educators, particularly pre-service teachers (Altınöz et al., 2019; Benzer & Karal, 2023; DSIT, 2024; Ravichandran et al., 2025). For instance, many Turkish educators feel inadequately prepared in cybersecurity and digital literacy (Altınöz et al., 2019), a sentiment echoed by observations of unconscious internet usage among intern teachers (Karagözlü, 2020). Turkish and international literature emphasizes that the "human factor" is critical in cybersecurity, with many security incidents resulting from human errors (IBM Corp, 2015; Colwill, 2010). Consequently, a widespread consensus exists on the imperative for global practical, continuous awareness training for teachers (Albrechtsen & Hovden, 2010; Eminağaoğlu, Uçar, & Eren, 2010; Akor et al., 2024). The beneficial effects of cybersecurity education in enhancing cyber resilience have been documented in various contexts (Al-Habashneh, 2023). However, a global challenge identified is the awareness-action gap, where individuals may have sufficient threat awareness but fail to adopt minimal preventive measures, a phenomenon observed in comparative studies including Türkiye (Zwilling et al., 2020).

Varied Influence of Demographic and Behavioral Factors

The role of demographic factors like gender on cyber awareness and behavior presents ambiguous results across studies. While a study in Jordan indicated higher cybersecurity awareness among male teachers (Al-Habashneh, 2023), this contrasts with meta-analysis and cyberbullying-focused research in Türkiye, finding negligible or no significant gender differences in general resilience or cyber sensitivity (Arı & Çarkıt, 2020; Çelik & Kaya, 2019). In contrast, other studies conducted with prospective teachers in Türkiye have found that men scored higher than women on digital competence and awareness scales (Kabataş Memiş, 2023; Sapanca & Kanbul, 2022). That output points to gender differences that are context-dependent or skill-dependent. This suggests that gender alone may not be the primary determinant of cyber resilience and that other factors, such as professional experience, quality of education, or specific digital competencies, may play a more important role.

On the other hand, studies conducted in Türkiye also reveal age-related differences; for example, older teachers generally show lower awareness and IT competencies compared to their younger colleagues (Canoğulları, 2021; Yayla, 2018; Durak & Seferoğlu, 2017; Demirer & Sak, 2015). On the other hand, another study found no significant difference in digital data security awareness based on overall years of professional experience (Yılmaz, Şahin, and Akbulut, 2016). Studies have also linked the frequency of internet use to awareness levels both in Türkiye and internationally (Sezer et al., 2015; Ahmed et al., 2021), but mere exposure does not guarantee preparedness (Sapanca & Kanbul, 2022), and problematic use can negatively impact focus and well-being (Gökmen et al., 2023; Satıcı, 2019).

Differences in Research Focus and Context

Studies in Türkiye differ in that they focus on the unique organization and recent changes in the national education system. Studies in Türkiye often examine educators' specific experiences with national initiatives such as the transition to distance education during the pandemic (Yılmaz & Karadağ, 2023; Güleç & Noyan, 2024; Bavli & Kortel, 2023; Adıgüzel et al., 2024) or their attitudes towards national platforms such as the National Education Information Network (EBA) (Düzgün, 2021). These studies tend to examine teachers' attitudes, perspectives, and technical/instructional challenges in this specific context in a more focused manner. On the other hand, global and international comparative studies usually aim to highlight the impact of cultural or systemic factors on awareness and behavior in different countries (e.g., Zwilling et al., 2020). International literature also focuses on the broader institutional security culture (Glaspie & Karwowski, 2018). In addition, there is a greater emphasis on implementing standardized risk management frameworks such as NIST CSF and ISO 27001 in academic settings (Alshar'e, 2023). Due to the impossibility of perfect prevention, studies abroad often conceptualize cyber resilience as an independent construct encompassing foresight, survival, recovery, and adaptation (Linkov et al., 2013; Linkov & Kott, 2018).

Joint Conclusion: The Critical Need for Training and Support

In general, studies conducted in Türkiye align with international reports on the general inadequacy of cybersecurity preparedness. On the other hand, methodological differences prevent direct comparison of general preparedness levels. Nevertheless, studies conducted in Türkiye provide valuable and context-specific findings regarding the challenges educators face adapting to digitalization within the national framework. Together, national and global studies aim to equip teachers with the necessary competencies and skills related to cybersecurity. Therefore, they jointly underline the need for more efficient, valuable, and continuous training. The outcomes of this training include important components such as evaluating online changes, understanding digital footprints, securing data access, safe SNS use, browser/email security, and reporting suspicious activities (Tomczyk et al., 2024; Adıgüzel et al., 2024; CISA, 2020). Therefore, according to the literature, providing resources and support such as workshops, online training, and peer networks is necessary. In this way, it will be ensured that teachers develop these skills and increase their self-efficacy (Bandura, 1994) and general cyber resilience (Sinclair & Wallston, 2004) in the increasingly complex digital learning environment. Based on these findings, this research will contribute to identifying which proactive and reactive skills should be focused on.

CHAPTER 3

METHODOLOGY

This chapter explains the study design, data collection tools and methods, study context, participant characteristics, and data analysis procedures.

3.1 Research Design

In this study, quantitative research approaches and a survey model are used to investigate primary school teachers' cyber resilience levels. Their cyber resilience levels were evaluated via a scenario-based instrument; then, answers given by teachers were quantified by two researchers using an analytical rubric. After reliable quantitative data were obtained, statistical analyses were performed to examine the distributions, differences, and relationships between various teacher characteristics. Table 3.1 summarizes the study's research questions, data sources, and analytical methods.

Table 3.1 Overview of Research Design

Research Question	Data Source	Analysis Method
RQ1: What is the distribution of teachers' overall cyber resilience scores and the scores for their sub-dimensions?	Cyber Resilience Scores	Descriptive Statistics
RQ2a: What is the difference in cyber resilience scores between teachers of different genders?	Cyber Resilience Scores & Demographic Information	Mann-Whitney U Test
RQ2b: What is the difference in cyber resilience scores between teachers who have received cybersecurity training and those who have not?	Cyber Resilience Scores & Demographic Information	Mann-Whitney U Test

Table 3.1 Continued

Research Question	Data Source	Analysis Method
RQ2c: What is the relationship between the duration of daily internet use and teachers' cyber resilience scores?	Cyber Resilience Scores & Behavioral Information	Kruskal Wallis H Test
RQ2d: What is the relationship between the frequency of digital tool use and teachers' cyber resilience scores?	Cyber Resilience Scores & Behavioral Information	Spearman Correlation
RQ2e: What is the relationship between years of professional experience and teachers' cyber resilience scores?	Cyber Resilience Scores & Demographic Information	Spearman Correlation

As seen in Table 3.1, this study was developed to examine the cyber resilience and sub-levels of primary school teachers. In addition, a quantitative research approach was conducted to examine how various characteristics relate to or affect these levels.

Survey design is commonly used in quantitative research to describe a population's tendencies, attitudes, or opinions by examining a sample of that population (Creswell & Creswell, 2018). This approach allows the researcher to quantitatively describe participants' opinions, attitudes, behaviors, and tendencies and produce generalizable findings based on data collected from a sample (Mertens, 2019). In survey research, cross-sectional and longitudinal designs are commonly used. Cross-sectional surveys collect data at one time to identify existing traits, while longitudinal surveys collect data over time to observe changes (Mertens, 2019). This study used the "Cyber Resilience Story Form for Teachers" tool, which was collected cross-sectionally. The form was used with convenience sampling. The complete answers of 192 out of 216 primary school teachers reached in Ankara in the spring of 2025 formed the basis of our study.

Questions were prepared to measure cyber resilience based on the five functions of the NIST CSF. A scenario-based form was developed since these functions focus on teachers' preventive and reactive solutions. Open-ended scenario questions were collected, scored with a created rubric, and converted into quantitative data. A normality test was performed with the help of the SPSS program (Kolmogorov-

Smirnov test, p < .05). The data were then statistically analyzed using non-parametric tests due to their non-normal distribution. As it shown in the Figure 3.1, these analyses allowed us to understand the level of general cyber resilience and its sub-levels (RQ1). In addition, it allowed us to investigate how teacher qualifications are related to this cyber resilience score or how they potentially affect it. Ethical approval was obtained (METU HREC, 21 January 2025, No: 0017-ODTUIAEK-2025), and participant consent was provided.

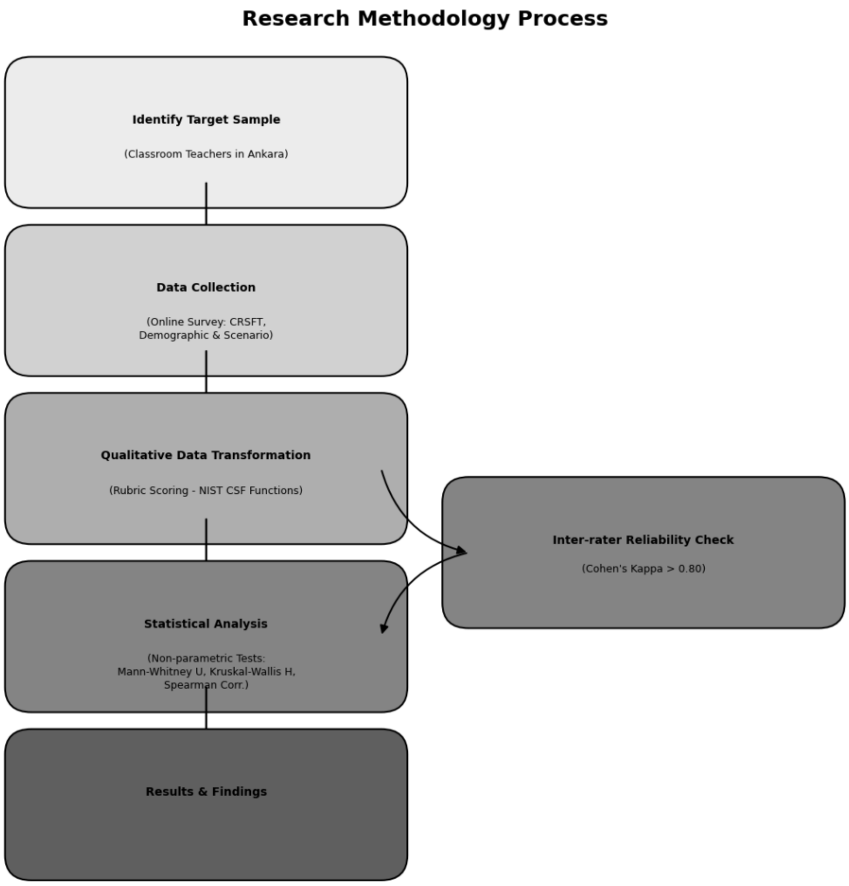


Figure 3.1 Research Methodology Process

3.2 Participants and Context

Teachers currently working in a public primary school in Ankara participated voluntarily in the survey. They were invited to participate through a Google Forms online survey invitation. A total of 192 primary school teachers participated in this study.

3.2.1 Sampling

Convenient sampling based on self-participation was used to locate the survey participants. The researchers sent an online survey to primary school teachers in public primary schools in Ankara. To conduct this research on a voluntary basis, the online survey included a notice about voluntary participation. Social media platforms and communication channels frequented by teachers were utilized to distribute the survey. This approach was adopted because it provided an easy and effective way to reach the target audience within the organization and within the defined geographical area of Ankara.

A total of 738 teachers initially participated in the survey. However, our study targeted primary school teachers, who are the first point of contact of students with technology in the school environment. As stated in the literature, primary school teachers play a crucial role in fostering cyber-resilient digital citizens for society. Therefore, primary school teachers were specifically targeted for this study. As a result, the sample was narrowed down to 216 primary school teachers. To ensure accurate cyber-resilience scores, participants who provided blank or incomplete responses were excluded from the analysis, resulting in a final sample size of 192 participants.

The sample consisted of 132 male (68.8%) and 60 female (31.2%) participants, reflecting the gender distribution typically observed in the Turkish education sector. The professional distribution of the participants mirrored the staffing pattern in schools, with 171 teachers (89.1%), 11 vice principals (5.7%), and 10 principles (5.2%).

Although the data of the participant group in the study was collected from Ankara, the capital city, its districts are considered representative of other less populated provinces throughout Türkiye. Therefore, the findings may provide insights applicable to the broader Turkish educational context. The final sample consisted of teachers who could be reached during the data collection period and who agreed to participate voluntarily, with an understanding that the convenience sampling approach has inherent limitations regarding generalizability.

3.2.2 Participants Characteristics

In the first part of the survey, items were prepared to collect participant demographic and behavioral characteristics. This section gathered data on gender, occupational position, and level of education. Participants were also asked about their years of teaching experience, whether they had previously attended any cybersecurity or digital security training programs, and their awareness of formal cybersecurity protocols within their schools. The survey further inquired about the digital tools, platforms, or software they most frequently use in their professional activities and their average daily internet usage time.

Demographic Information

In this study, 192 primary school teachers working in public schools in Ankara participated. Demographic characteristics are presented in Table 3.2.

Table 3.2 Distribution of Participants by Gender, Education Level and Position

Category	**Sub-category/variable**	**Frequency (N)**	**Percentage (%)**
Gender	Male	60	31.2
	Female	132	68.8
Occupational Position	Teacher	171	89.1
	Principle	10	5.2
	Assistant Manager	11	5.7
Level of Education	Master's Degree	30	15.6
	Doctorate Degree	1	0.5
	Bachelor’s Degree	161	83.9
Total		192	100.0

Table 3.2 shows that 60 (31.2%) of the 192 teachers who participated in the study were men, while 132 (68.8%) were women. When their graduation status was assessed, 161 participants (83.9%) had a bachelor's degree, 30 (15.6%) had a master's degree, and 1 (0.5%) had a doctorate degree. Most of the participants (n=171, 89.1%) were teachers, with 10 (5.2%) serving as principals and 11 (5.7%) as assistant principals.

Cybersecurity Training and School Policy

Table 3.3 shows teachers' level of awareness of cyber security policies in their schools and whether they have received cyber security training.

Table 3.3 Participants' Reported Awareness of School Cybersecurity Policy and Prior Cybersecurity Training

Category	**Response**	**Frequency (n)**	**Percentage (%)**
Cybersecurity Policy	Yes	57	27.9
	No	29	15.1
	Unsure / No Opinion	106	55.2
Cybersecurity Training Received	Yes	35	18.2
	No	157	81.8
Total		192	100

According to Table 3.3 29.7% (n=57) of the participants said their schools had a cybersecurity policy, while 15.1% (n=29) said they didn't. However, it is noteworthy that more than half of the participants (55.2%, n=106) stated that they were unaware of the school policy ("I have no idea"). When the status of receiving cybersecurity training is examined, it is revealed that the vast majority of participants (81.8%, n=157) did not receive any training on the subject. The percentage of those who said they received training is 18.2% (n=35).

Digital Tools and Software Used

The most frequently used digital tools and software by teachers are presented in Table 3.4.

Table 3.4 Frequency of Mention for Commonly Used Digital Tools and Software by Participants

Category	**Tool/software Example**	**Frequency (N)**
Digital Tool/Software Usage	Smart Board	155
	Computer (Laptop/Desktop)	98
	Microsoft Office Suite	64
	Phone (Smartphone)	57
	EBA (Education Info. Network)	48
	Operating Systems	22

Table 3.4 depicts how the participants used digital tools and software. The analysis (N=192) shows that the Smart Board is the most used tool among the participants, with 80.7% (n=155) stating that they used it. Computers are ranked second with a usage rate of 51.0% (n=98). These are followed by Microsoft Office Programs (n=64, 33.3%), Phone (n=57, 29.7%), and Education Information Network (n=48, 25.0%). Other tools mentioned less frequently are operating systems (n=22, 11.5%), Google Tools (n=19, 9.9%), and Canva (n=16, 8.3%). The number of digital tools or applications used per teacher is given in Table 3.5

Table 3.5 Number of the Digital Tools and Applications Used by Teachers

Number Of Digital Tools/applications Used	**Frequency (N)**	**Percentage (%)**
0	4	2.1%
1	20	10.4%
2	55	28.6%
3	39	20.3%
4	44	22.9%
5	16	8.3%
6	7	3.6%
7	3	1.6%
8	1	0.5%
9	3	1.6%
Total	192	100.0%

Table 3.5 shows how the participants used digital tools and software. According to the analysis of 192 people, the most frequent number of tools used is 2 (28.6%; n=55). Usage of 4 tools comes in second place (22.9%; n=44). This is followed by 3 tools (20.3%; n=39), 1 tool (10.4%; n=20), and 5 tools (8.3%; n=16). Usage of 8 tools (0.5%; n=1), 7 tools (1.6%; n=3), 9 tools (1.6%; n=3), and 0 tools (2.1%; n=4) are among the numbers of tools with the least use.

Daily Internet Usage Duration

Teachers' daily internet usage time is presented in Table 3.6.

Table 3.6 Distribution of Participants by Self-Reported Average Daily Internet Usage Duration

Category	Usage Duration (Hours per day)	Frequency (n)	Percentage (%)
Daily Internet Usage	Under two hours	104	54.2
	Between two and four hours	65	33.8
	More than four hours	23	12.0
Total		192	100

Table 3.6 shows how the participants' daily internet usage durations were divided into three different groups. The table shows that more than half of the participants (n=104, 54.2%) spend 0-2 hours per day on the internet. This is followed by those who use it for 2-4 hours per day, with a 33.9% rate (n=65). Participants who use the internet for more than 4 hours per day have the lowest rate, at 12.0% (n=23). This grouping demonstrates that most participants spend their time on the internet for shorter periods.

Teaching Experience

Table 3.7 shows the distribution of the duration of professional experience of the teachers participating in the study.

Table 3.7 Distribution of Participants by Years of Professional Teaching Experience

Category	**Experience Range (Years)**	**Frequency (N)**	**Percentage (%)**
Experience Years	5-9	13	6.8
	10-14	23	12.0
	15-19	32	16.7
	20-24	42	21.9
	25-29	50	26.0
	30-34	22	11.5
	35-39	10	5.1
Total		192	100

Table 3.7 shows that when the participants' years of professional experience are examined, the densest concentration is found between 25-29 years (%26.0) and 20-24 years (%21.9). These groups are followed by those with 15-19 years' experience (%16.7). Participants with 10-14 years (%12.0) and 30-34 years (%11.5) of experience have similar rates. While the rate of participants with less experience in the 5-9 year range is 6.8%, the lowest rate is seen in the most experienced group, the 35-39 year range, at 5.2%. This distribution reveals that a sizable proportion of the research group (%64.6 with 15-29 years of experience) has professional experience.

3.3 Data Collection Instruments

The primary data collection tool used in this study was the Cyber Resiliency Story Form for Teachers (CSRFT), which was developed for this research. Cyber resilience requires reactive skills, and this tool was developed specifically to both measure these and integrate the five core functions of the NIST CSF. In other words, there was no scale in the literature that addressed both the cyber resilience scale and the use of the NIST CSF within the educational context. This tool was designed to examine two main dimensions: first, teachers’ digital resilience in the context of cybersecurity risks, and second, their use of digital educational tools in their teaching practices. The CRSFT is divided into two main sections to capture both background information and behavioral responses comprehensively. The first section focuses on the demographic characteristics of the participants, including professional experience, previous cybersecurity training, and the use of digital technologies in educational settings. The second section offers a scenario-based approach where participants are presented with a hypothetical cyber threat situation. Furthermore, the scenario asks them to respond to open-ended questions about how they would behave in such a situation. In other words, this section is designed to obtain qualitative data on teachers’ resilience-related behaviors, coping strategies, and decision-making processes when faced with cybersecurity challenges. The development of the instrument was informed by the core functions of the NIST CSF; thus, the questions and scenario items in the tool were aligned with the NIST CSF. The combination of structured quantitative items and open-ended qualitative prompts aimed to provide a holistic understanding of teachers’ levels of cyber resilience.

According to this, the first part of the CRSFT focused on collecting background and demographic data through closed-ended quantitative questions, such as gender, educational level, years of teaching experience, and current role, including teacher or principal. Moreover, it focused on their engagement with digital technologies. For example, the digital tools or software they use most frequently and average daily internet usage. Additionally, participants were asked about their previous participation in seminars, workshops, or training programs concerning digital safety and cybersecurity. The purpose of this section was to contextualize the participants' responses within their individual and professional characteristics, offering a baseline understanding of their digital engagement and prior exposure to cybersecurity education.

Table 3.8 List of Data Collection Instruments

Tool/method	Description And Purpose
Cyber Resilience Story Form for Teachers	Developed by researchers to evaluate teachers' digital resilience concerning the use of digital education tools and cybersecurity. It consists of two sections: 1) Demographic, professional, and digital usage information; 2) Scenario-based open-ended questions aligned with NIST CSF functions.
Analytical Rubric	A scoring tool developed based on NIST CSF functions to convert open-ended scenario responses from the second section of the Story Form into numerical data (scores ranging from 0-3).

Table 3.8 shows the list of data collection instruments used in the research. Our study created a rubric based on NIST CSF functions to evaluate teachers' cyber resilience levels. While making the rubric, rubric studies for teachers were used (e.g., Yaman, Bal & Sarışan, 2024). The rubric includes performance criteria rated 0 (insufficient) and 3 (high level) for each function. This is because evaluating multiple options in the social sciences is challenging. After collecting the responses of the teachers to scenario-based open-ended questions, numerical data were obtained by scoring them with the help of the created rubric (Hochwald et al., 2023). Cohen's Kappa coefficient is a statistical measure of the agreement between two raters, and values above 0.80 indicate high consistency (Cohen, 1960). In this context, the two researchers scored separately and used Cohen's Kappa coefficient to analyze the rater consistency. As a result, the findings show reliability.

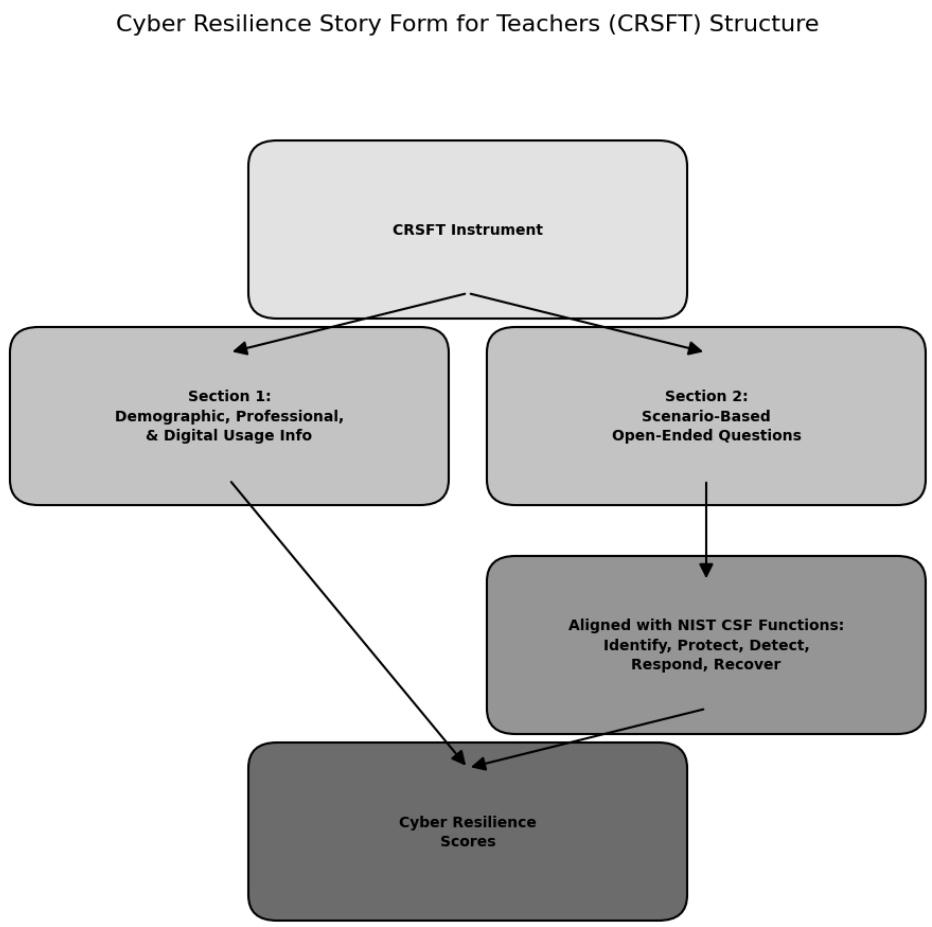


Figure 3.2 Cyber Resilience Story Form for Teachers (CRSFT) Structure

3.3.1 Scenario-Based Cyber Resilience Assessment

As shown in the Figure 3.2, the tool's content presented to measure the cyber resilience levels of the participants is mentioned. Since cyber resilience skills are based on reactive and proactive activities, a different method had to be followed to measure the behaviors; accordingly, we prepared a scenario to see the teachers' functioning in our study. We prepared a realistic ransomware attack scenario in an everyday classroom environment. Then, the participants were asked questions to reveal their expected reactions, thought processes, and coping strategies in the face of such a cyber incident.

These scenario-based questions were designed based on the five basic functions of the NIST CSF. Each function has a meaning related to various aspects of cyber resilience. The scenario has two questions for each function, one of which is reinforcement. Below, it is stated how the NIST CSF functions to measure cyber resilience.

Identify: This measure measures teachers' awareness of risky data types and potential risks associated with ransomware attacks.

Protect: Assessed participants' preventive measures, including data and file protection practices and backup strategies.

Detect: Focused on identifying early warning signs and participants' diagnostic skills when faced with a cybersecurity threat.

Respond: Examined participants' reactive action steps when they detected a ransomware incident.

Recover: Assessed participants' understanding of recovery procedures, including post-attack data recovery, safe return to operation, and learning from the attack.

Therefore, a scenario-based survey was designed to collect qualitative data on participants' practical problem-solving skills and procedural knowledge of cyber threats.

3.3.2 Instrument Adaptation and Validity

The CRSF for teachers was meticulously and explicitly developed for this study. To ensure content validity, the open-ended questions in the scenario were created by incorporating the five functions of the NIST CSF, which represent cyber resilience skills. In this context, other scenario-based tools used in the field of education and cybersecurity were examined. Expert consultation was obtained from academics and professionals specialized in both cybersecurity and education. They also contributed to the improvement of the tool's content and structure. Before the main study was implemented, the tool underwent a pilot test phase with a small group of teachers. The feedback obtained during this phase facilitated further revision and optimization of the questions. These observations and revisions increased the clarity and effectiveness of the questions. It was observed that the expected completion time for the entire forum was between 10 and 15 minutes.

3.4 Data Collection Procedure

The data collection process of this study was conducted through an online survey. It was designed and responses were managed through Google Forms. Information about the study, the volunteer form, and the survey link of the study were sent to potential participants together. This was done through institutional communication channels and direct e-mail invitations. Data were collected in the spring semester of the 2025 academic year, and participants reported that the survey took approximately 10 to 15 minutes to complete.

During the data collection process, special attention was paid to ethical issues to ensure compliance with research standards. The study received official approval from the Middle East Technical University Human Research Ethics Committee (IAEK) on January 21, 2025 (Approval Number: 0017-ODTUIAEK-2025). Before participation, all participants were sent an electronic informed consent form outlining the purpose of the study, the voluntary nature of participation, and their rights as research participants. Only participants who were informed and gave their consent were allowed to continue with the survey.

The confidentiality and anonymity of the participants were meticulously protected throughout the research process. All data collected was securely stored. Additionally, they were used only for the purposes of this study and in accordance with approved ethical guidelines.

3.5 Data Analysis

The data analysis process of the study is designed to accurately interpret the collected data in relation to the research objectives. In other words, data were collected in two stages, both closed and open-ended items. Therefore, the transformation method was employed to analyze both quantitative and qualitative data simultaneously. In this context, it was planned to systematically transform qualitative responses into quantitative points, and a rubric was developed. In this context, the analysis proceeded in three main stages to achieve research goals. First, the qualitative responses were graded based on the rubric. Later, the reliability of the scoring was evaluated using Cohen's Kappa coefficient to assess inter-evaluator agreement. Finally, appropriate statistical analyses were applied to examine the relationships between the main variables using IBM SPSS 27 software.

Table 3.9 Normality Test of Cyber Resilience Overall and Dimension

Variable	**Mean**	**Sd**	**Skewness**	**Se (Skew)**	**Kurtosis**	**Se (Kurt)**	**Sig.**
Identify	1.610	1.244	.497	.175	-.354	.349	<.001
Protect	2.510	1.298	-.349	.175	.251	.349	<.001
Detect	2.700	1.041	.634	.175	-.455	.349	<.001
Respond	2.090	1.251	.205	.175	-.292	.349	<.001
Recover	1.470	1.587	-.784	.175	.867	.349	<.001
Cyber Resilience Score	9.090	4.028	-.293	.175	-.249	.349	.003

The descriptive statistics are summarized in Table 3.9. To evaluate whether the assumptions of normality, homogeneity, and low intercorrelations were satisfied, descriptive statistics were calculated, including the mean, standard deviation, minimum and maximum values, range, skewness, kurtosis, and the results of the Kolmogorov-Smirnov normality test.

3.5.1 Qualitative Data Transformation (Rubric Scoring)

One of the main components of data analysis included systematic transformation for statistical evaluation. In other words, it was planned to systematically transform qualitative responses into quantitative data for measurements. In this process, teachers' verbal responses to open-ended questions in CRSF were used. For this purpose, a specially designed rubric developed specifically for this study was used. The rubric was structured according to the five basic functions of NIST CSF. Specific sample answers and their scores were prepared for each task. In other words, participants' responses were scored on a four-point scale ranging from 0 for inadequate performance to 3 for excellent performance or understanding. This criterion-based scoring approach ensured that qualitative descriptions were systematically and reliably transformed into numerical data. The scoring methodology was implemented by utilizing established practices for transformation (Hochwald et al., 2023).

3.5.2 Inter-rater Reliability (Cohen's Kappa)

To ensure the objectivity and consistency of the scoring process, two independent researchers evaluated the qualitative responses using the developed rubric. The degree of agreement between researchers was assessed through the calculation of Cohen's Kappa coefficient (Cohen, 1960). The resulting Kappa value exceeded 0.80 ($\kappa > 0.80$), indicating a high level of inter-rater reliability and confirming the consistent application of the scoring criteria throughout the data evaluation process.

3.5.3 Statistical Analyses

Before statistical analyses were conducted, the normality of quantitative data, including outcome-based scores, was assessed using the Kolmogorov-Smirnov test showed in Table 3.10. Accordingly, the total cyber resilience scores and most subscales did not show normality ($p < .05$), indicating that the studies violated the assumptions required for parametric testing.

Table 3.10 Tests of Normality for Study Variables Kolmogorov–Smirnov

Variable	Kolmogorov–smirnov Statistic	Df	P
Identify	.177		<.001
Protect	.242		<.001
Detect	.259		<.001
Respond	.170		<.001
Recover	.235		<.001
Cyber Resilience Score	.082	192	.003

According to table 3.10, The Shapiro–Wilk test was not used because the sample size was over 50. The cyber resilience total score and its sub-dimensions do not show a normal distribution according to the Kolmogorov–Smirnov test ($p<0.05$).

Given these findings, nonparametric statistical methods were used in subsequent analyses. These included appropriate techniques for group comparisons and correlation analyses. These analysis methods were consistent with the dataset's distributional properties and the study's methodological rigor.

Analysis Used

Table 3.11 shows the research questions and statistical analysis used on the variables.

Table 3.11 Research Questions and Statistical Analysis Used

Research Question	Statistical Analysis
RQ1: What are the descriptive statistics (e.g., mean, standard deviation, and median) for teachers' overall cyber resilience scores and each of their five sub-dimensions?	Descriptive Statistics (Frequency, Percentage, Mean, Standard Deviation, Median)
RQ2a: What is the difference in cyber resilience scores between teachers of different genders?	Mann-Whitney U Test

Table 3.11 Continued

Research Question	Statistical Analysis
RQ2b: What is the difference in cyber resilience scores between teachers who have received cybersecurity training and those who have not?	Mann-Whitney U Test
RQ2c: What is the relationship between the duration of daily internet use and teachers' cyber resilience scores?	Kruskal Wallis H Test
RQ2d: What is the relationship between the frequency of digital tool use and teachers' cyber resilience scores?	Spearman Correlation
RQ2e: What is the relationship between years of professional experience and teachers' cyber resilience scores?	Spearman Correlation

As shown in Table 3.11. The Mann-Whitney U test and Kruskal-Wallis H test were used to compare independent groups, and the Spearman correlation coefficient was used to examine the relationship between ordinal variables.

CHAPTER 4

RESULTS

This section presents the answers for the research questions of the study. It begins with statistical test results on the teachers' cyber resilience scores. Demographic information including gender, cybersecurity training status, and daily internet usage time will be provided descriptively. The results regarding the observed differences in cyber resilience scores will be presented. The findings regarding the relationships between cyber resilience scores and variables such as digital tool/software use and professional experience will be presented lastly.

Descriptive statistics were computed to provide a foundational understanding of the teachers' cyber resilience scores in the study (N=192). This included examining the overall resilience scores, the specific scores associated with each of the five core functions, and the NIST CSF.

4.1.1 Overall Cyber Resilience Scores

Table 4.1 shows descriptive statistics calculated to reveal the general cyber resilience scores of 192 teachers who participated in the study, as well as their status in the cyber resilience sub-dimensions to answer RQ1 "**RQ1:** What is the distribution of teachers' overall cyber resilience scores and the scores for its sub-dimensions?". Thus, we will be able to observe teachers' attitudes towards cyberattacks.

Table 4.1 Descriptive Statistics on Teachers' Overall Cyber Resilience Scores and Sub-Dimensions of Cyber Resilience

Csf Dimension	Mean (M)	Standard Deviation (Sd)	Median	Minimum	Maximum
Overall Cyber Resilience	8.67	4.028	9.00	1	20
Identify	1.61	1.244	2.00	0	5
Protect	2.68	1.139	3.00	0	5
Detect	0.91	0.922	1.00	0	4
Respond	1.90	1.251	2.00	0	5
Recover	1.57	1.587	1.00	0	6

As shown in Table 4.1 and Figure 4.1, the participants' average cyber resilience score was 8.67 (SD = 4.028). The highest mean score for cyber resilience sub-dimensions is Protection (M = 2.68, SD = 1.139) as it is shown in Figure 4.3. Other dimensions have mean and standard deviation values of Responding (M = 1.90, SD = 1.251) as it is shown in Figure 4.5, Identification (M = 1.61, SD = 1.244) as it is shown in Figure 4.2, and Recovery (M = 1.57, SD = 1.587) as it is shown in Figure 4.6, respectively. The dimension with the lowest mean score was Detection (M = 0.91, SD = 0.922) as it is shown in Figure 4.4. When median values are examined, it is seen that the dimensions of Protection (Med=3.00), Responding (Med=2.00), and Identification (Med=2.00) are higher than the average. The median for the Detection dimension was slightly higher than its mean (M=0.91), whereas the median for the Recovery dimension was notably lower than its mean (M=1.57). Previous normality tests, as well as Kolmogorov-Smirnov and skewness-kurtosis tests, revealed that both the overall cyber resilience score and the overall distributions of all sub-dimension scores deviated significantly from normal.

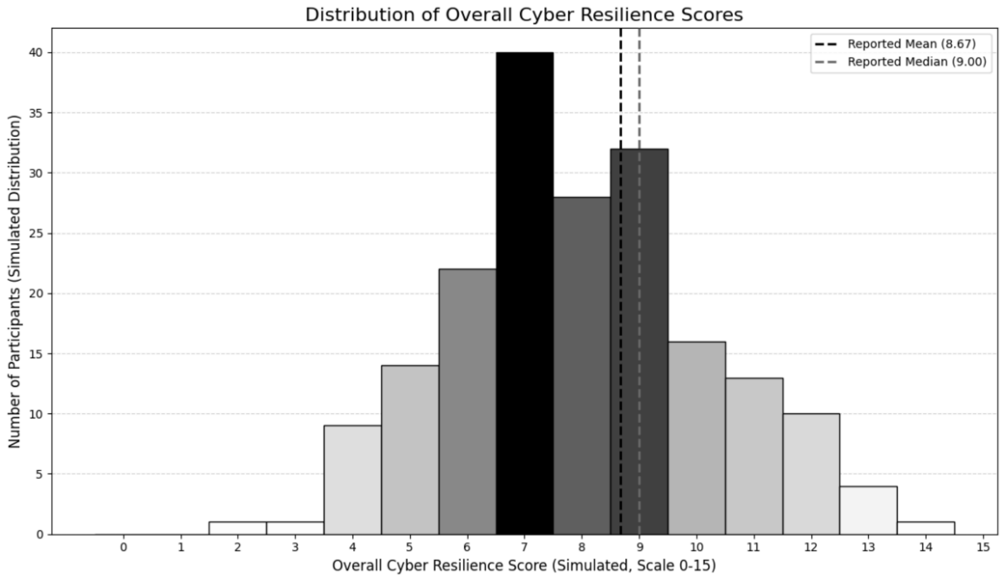


Figure 4.1 Distribution of Overall Cyber Resilience Scores

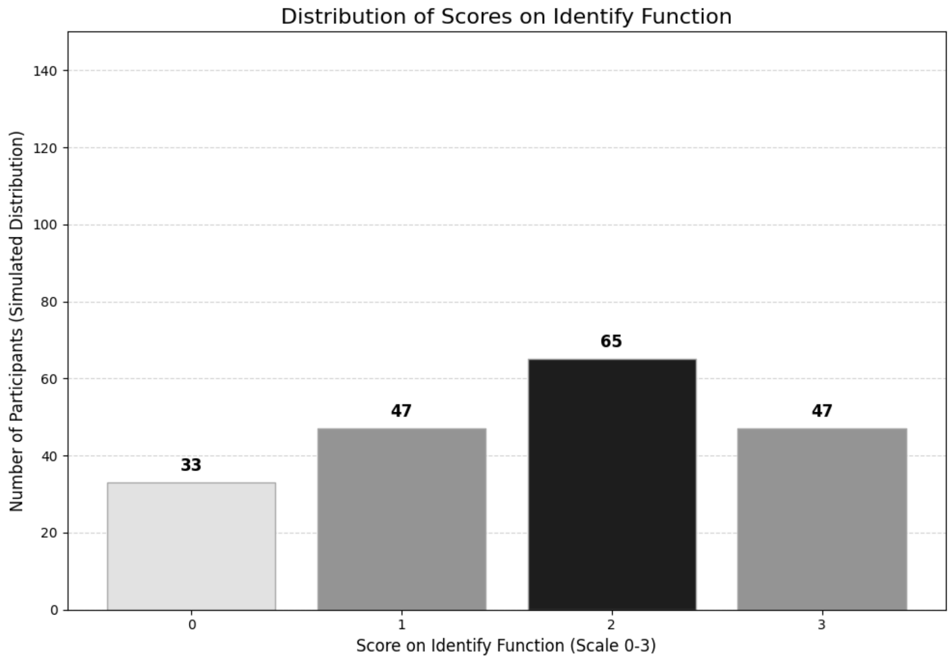


Figure 4.2 Distribution of Scores on Identify Function

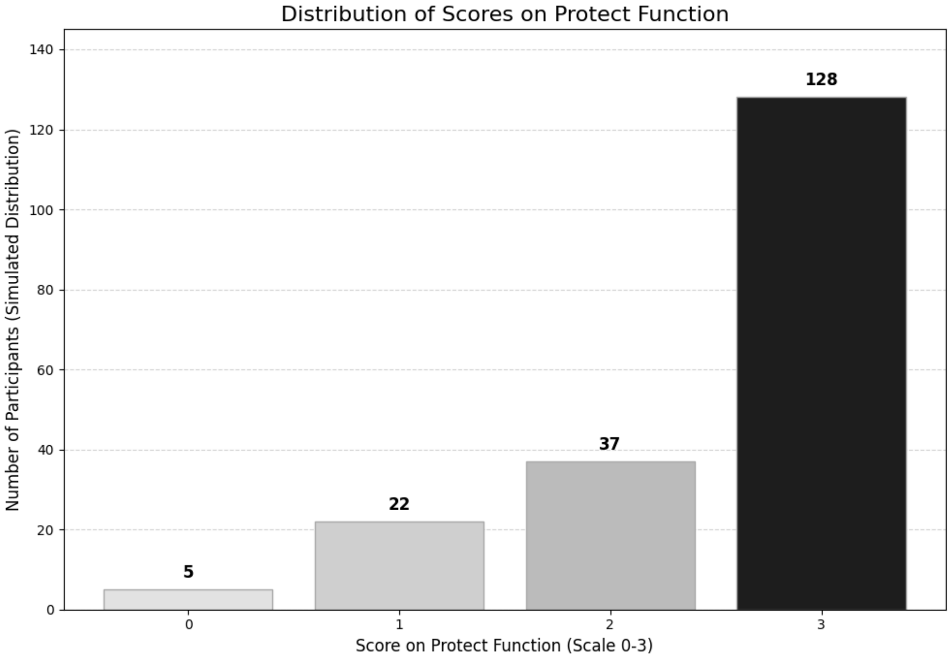


Figure 4.3 Distribution of Scores on Protect Function

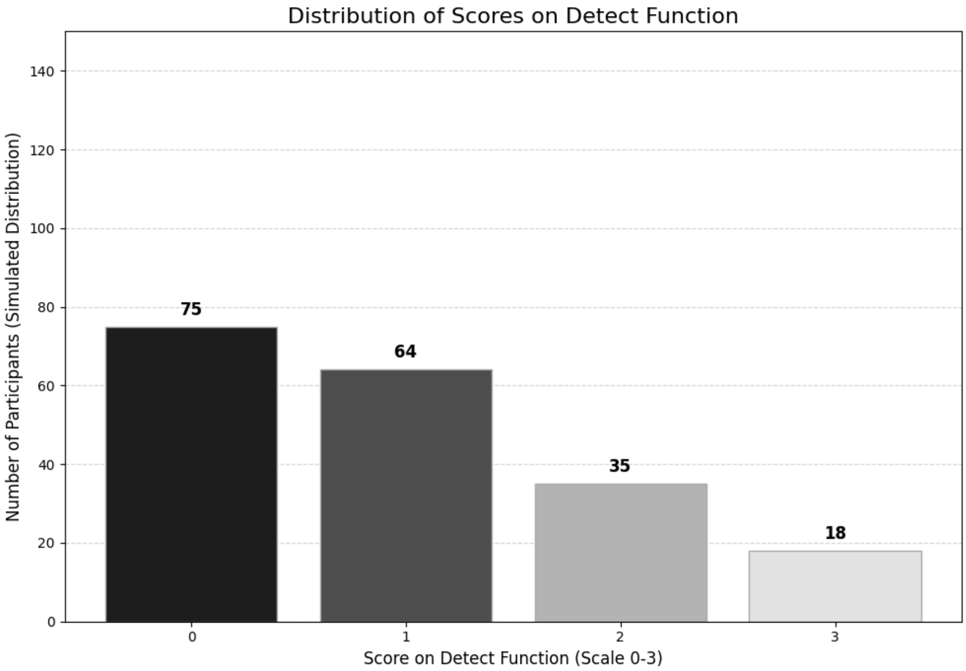


Figure 4.4 Distribution of Scores on Detect Function

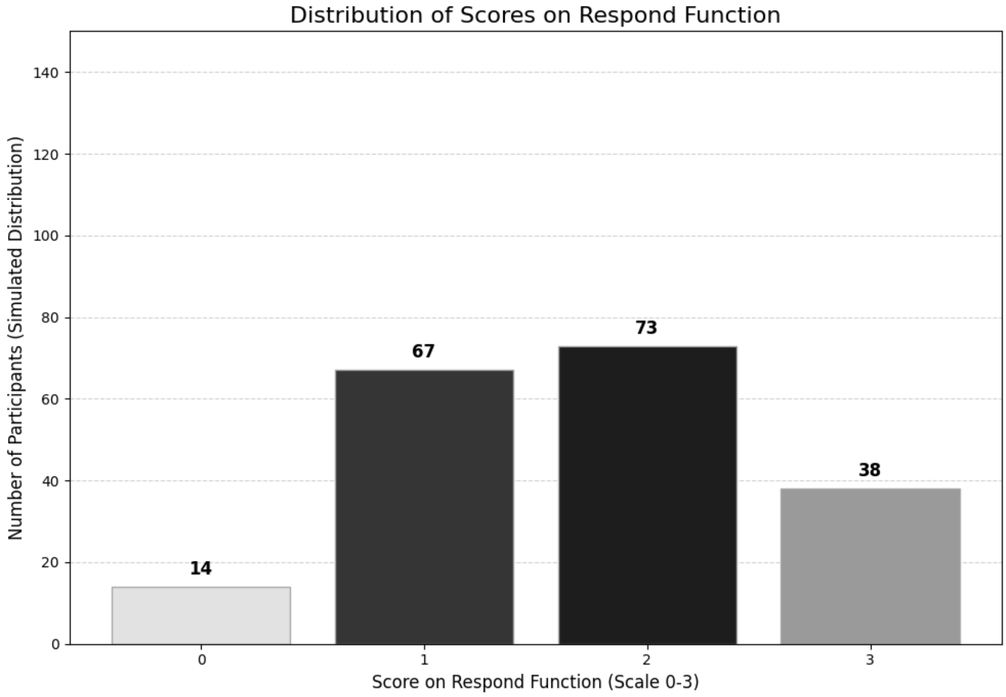


Figure 4.5 Distribution of Scores on Respond Function

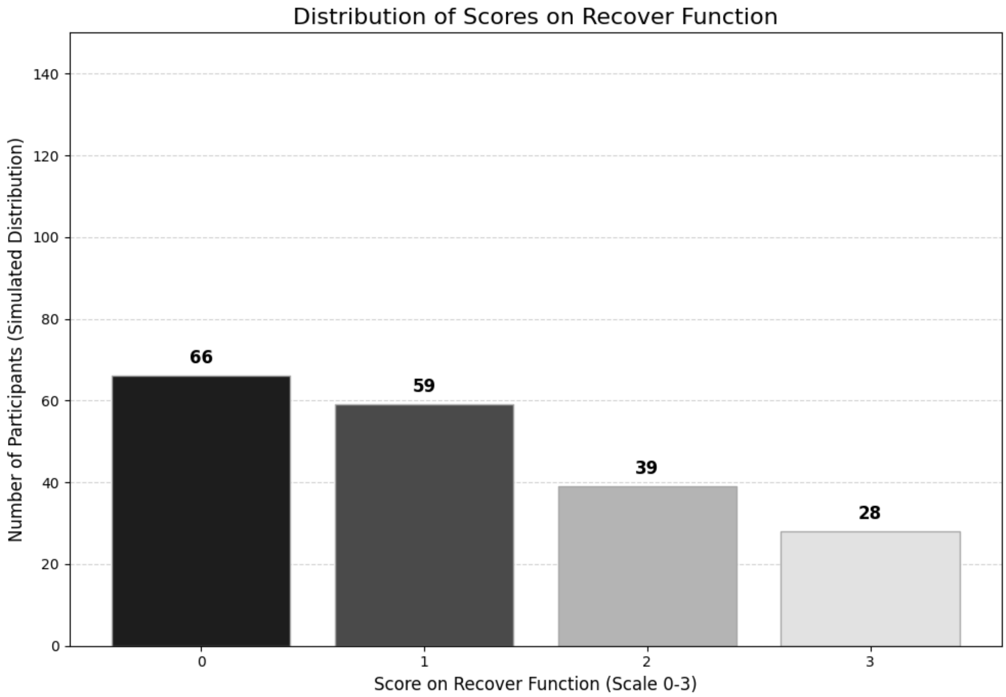


Figure 4.6 Distribution of Scores on Recover Function

4.2 Findings Regarding Differences in Cyber Resilience Scores

Mann-Whitney U tests and Kruskal-Wallis H are used, since the assumptions for normality are not met, to check if groups' levels of cyber resilience vary. The comparison of cyber resilience scores between teacher genders and those who report prior cybersecurity training is explained in the section that follows.

4.2.1 Gender Differences

Addressing the research question, "To what extent do demographic and behavioral variables, gender, digital tool competencies, daily internet use, professional competencies, and whether or not to receive cyber security training affect teachers' cyber resilience levels?", the study examined several factors. Regarding the role of gender in particular, Table 4.2 shows the results of the Mann-Whitney U test, which was used to see if teachers' cyber resilience scores differed by gender. In this way we will see if the overall lifestyle has an impact.

Table 4.2 Mann-Whitney U Test Results for Cyber Resilience Scores by Gender

CR Score	Gender	N	Median	Mean Rank	Mann-whitney U	Z	P
Total Cyber Resilience	Female	132	8	86.96	2700.500	-3.539	<.001
	Male	60	10	117.49			
Identification	Female	132	8	90.36	3149.000	-2.341	.019
	Male	60	10	110.02			
Protection	Female	132	8	88.61	2918.500	-3.080	.002
	Male	60	10	113.86			
Detection	Female	132	8	86.73	2671.000	-3.839	<.001
	Male	60	10	117.98			

Table 4.2 Continued

CR Score	Gender	N	Median	Mean Rank	Mann-whitney U	Z	P
Response	Female	132	8	94.52	3699.000	-0.751	.453
	Male	60	10	100.85			
Recovery	Female	132	8	89.97	3097.500	-2.513	.012
	Male	60	10	110.88			

As Table 4.2 illustrates, the cyber resilience scores of 60 male and 132 female teachers were compared using the Mann-Whitney U Test. The comparison revealed a statistically significant difference between the two groups' overall cyber resilience scores ($U = 2700.500$, $Z = -3.539$, $p < .005$). Overall cyber resilience scores were higher for male teachers than for female teachers. This is supported by mean ranks and demonstrated by the median scores (female median = 8.00, male median = 10.00) as it shown in Figure 4.7.

Further examination at the NIST CSF sub-dimension level revealed that this pattern persisted across numerous functions. For the Identify ($Z = -2.341$, $p = .019$), Protect ($Z = -3.080$, $p = .002$), Detect ($Z = -3.839$, $p < .005$), and Recover ($Z = -2.513$, $p = .012$) functions, there were statistically significant differences, with male educators having higher scores. However, there was no gender-related statistically significant difference in the Respond function ($U = 3699.000$, $Z = -0.751$, $p = .453$).

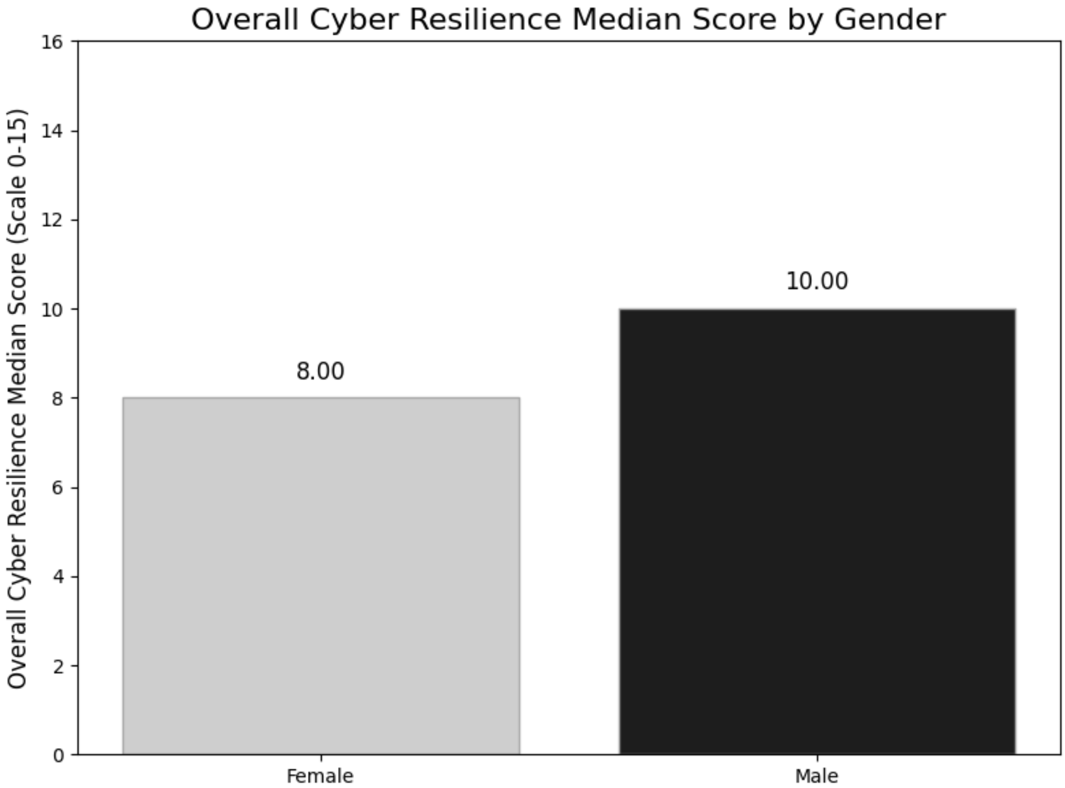


Figure 4.7 Overall Cyber Resilience Median Score by Gender

4.2.2 Differences Based on Cybersecurity Training

To investigate the research question, “To what extent do demographic and behavioral variables, gender, digital tool competencies, daily internet use, professional competencies, and whether or not to receive cybersecurity training affect teachers' cyber resilience levels?”, the study examined the impact of various factors. Focusing on the effect of Cyber Security Training Status, the Mann-Whitney U test was used to compare the Cyber Resilience Scores of Teachers based on whether they had received training. Table 4.3 displays the results. Therefore, we will realize the value of having an education on the subject.

Table 4.3 Mann-Whitney U Test Results: Cyber Resilience Scores by Cybersecurity Training Status

Cybersecurity Training Group	**N**	**Mean Rank**	**Mann-whitney U**	**Wilcoxon W**	**Z**	**P**
No Training	157	91.85				
Had Training	35	117.36	2017.50	14420.50	-2.463	.014

According to the analysis results shown in Table 4.3, the mean rank of cyber resilience scores among teachers who did not receive cyber security training (Group 1: No, n = 157) was 91.85. The mean rank of cyber resilience scores among teachers who received cyber security training (Group 2, n = 35) was 117.36. The Mann-Whitney U test result revealed a statistically significant difference in cyber resilience scores between the two groups ($U = 2017.500$, $Z = -2.463$, $p=.014$). As shown in the Figure 4.8, teachers who received cyber security training showed significantly higher cyber resilience scores (mean rank = 117.36) compared to those who did not (mean rank = 91.85) ($p<.05$).

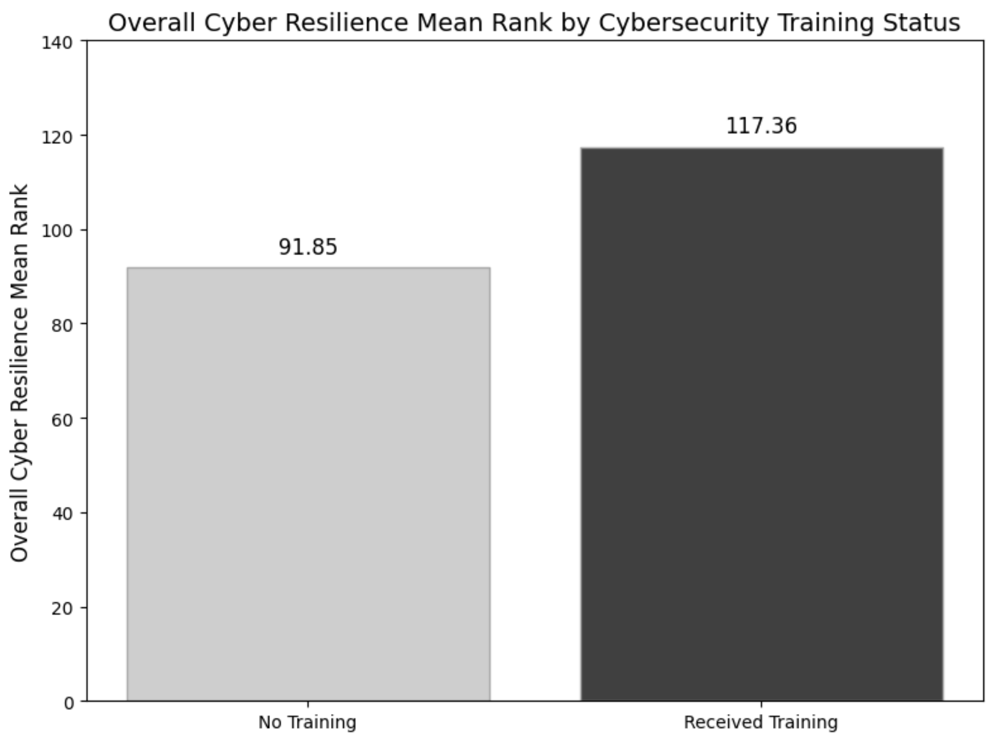


Figure 4.8 Overall Cyber Resilience Mean Rank by Cybersecurity Training Status

4.2.3 Differences Based on Daily Internet Usage Duration

To investigate the research question, "To what extent do demographic and behavioral variables, gender, digital tool competencies, daily internet use, professional competencies, and whether or not to receive cyber security training affect teachers' cyber resilience levels?", the Kruskal-Wallis H Test was used to compare teachers' cyber resilience scores to their daily internet usage time, and the results are shown in Table 4.4. In that case, we will see the impact of daily habits such as time spent on the computer.

Table 4.4 Kruskal-Wallis H Test for Teachers' Cyber Resilience Scores by Daily Internet Usage Duration

Group	**N**	**Median**	**Mean Rank**	**Kruskal-wallis H**	**Df**	**P**
Lower than 2 hours	104	9	97.33			
Between 2 and 4 hours	65	8	90.20			
More than 4 hours	23	9	110.57			
Total	192	9				
Kruskal-Wallis H				2.346	2	.309

As it is shown in the Table 4.4, the Kruskal-Wallis H test was used to see if there was a significant difference in total cyber resilience scores between the teachers' daily internet usage duration groups (0-2 hours, 2-4 hours, and 4+ hours). The analysis results revealed that there was no statistically significant difference in cyber resilience scores between internet usage duration groups ($H(2) = 2.346$, $p = .309$). As it shown in the Figure 4.9, then the mean ranks of the groups were examined (0-2 hours: 97.33, 2-4 hours: 90.20, 4+ hours: 110.57), no significant or statistically significant rank difference was found between the groups. The Median test revealed no significant difference between group medians ($\chi^2(2) = 0.171$, $p = .918$), supporting this finding.

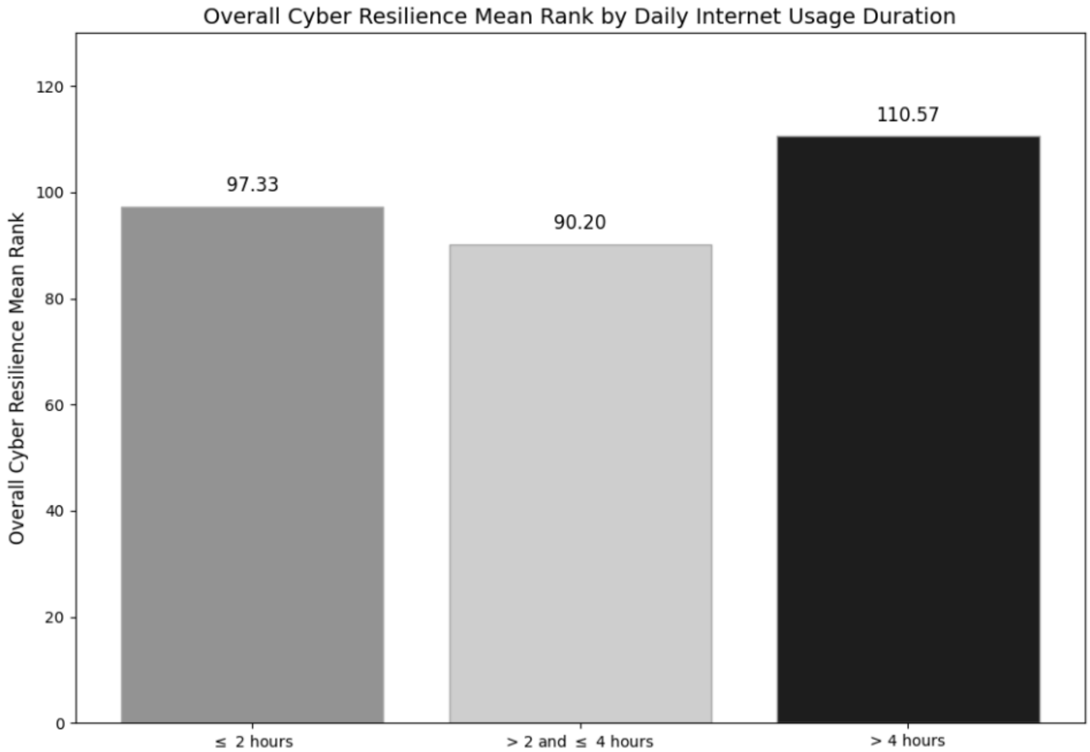


Figure 4.9 Overall Cyber Resilience Mean Rank by Daily Internet Usage Duration

4.3 Findings Regarding Relationships with Cyber Resilience Scores

The relationship between teachers' cyber resilience scores and the value of digital tools and teaching work experience is examined in this section. Using the Spearman correlation, since the assumptions for normality are not met, was computed to look for monotonic relationships.

4.3.1 Correlation with Digital Tool/Software Usage

To address the research question, "To what extent do demographic and behavioral variables, gender, digital tool competencies, daily internet use, professional competencies, and whether or not to receive cyber security training affect teachers' cyber resilience levels?", a series of analyses were conducted. As part of this investigation, Spearman Table 4.5 displays the results of a correlation analysis to determine the relationship between teachers' cyber resilience scores and their use of digital tools and software. Thus, we will be able to examine the impact of their competence in using technology on the subject.

Table 4.5 Spearman Correlation Between Teachers' Cyber Resilience Scores and Digital Tool/Software Usage

			Number of Digital Tools Used	Cyber Resilience Score
Spearman's rho	**Number of Digital Tools Used**	Correlation Coefficient	1,000	,191
		Sig. (2-tailed)	.	,008
		N	192	192
	Cyber Resilience Score	Correlation Coefficient	,191	1,000
		Sig. (2-tailed)	,008	.
		N	192	192

Table 4.5 and Figure 4.11, shows a weak positive and significant correlation between teachers' use of digital tools and software and their cyber resilience scores (ρ =.191, p =.008, N = 192). This finding and the Figure 4.10 that is grouped digital tool use numbers into five, indicates that as the use of digital tools and software increases, cyber resilience scores tend to rise slightly.

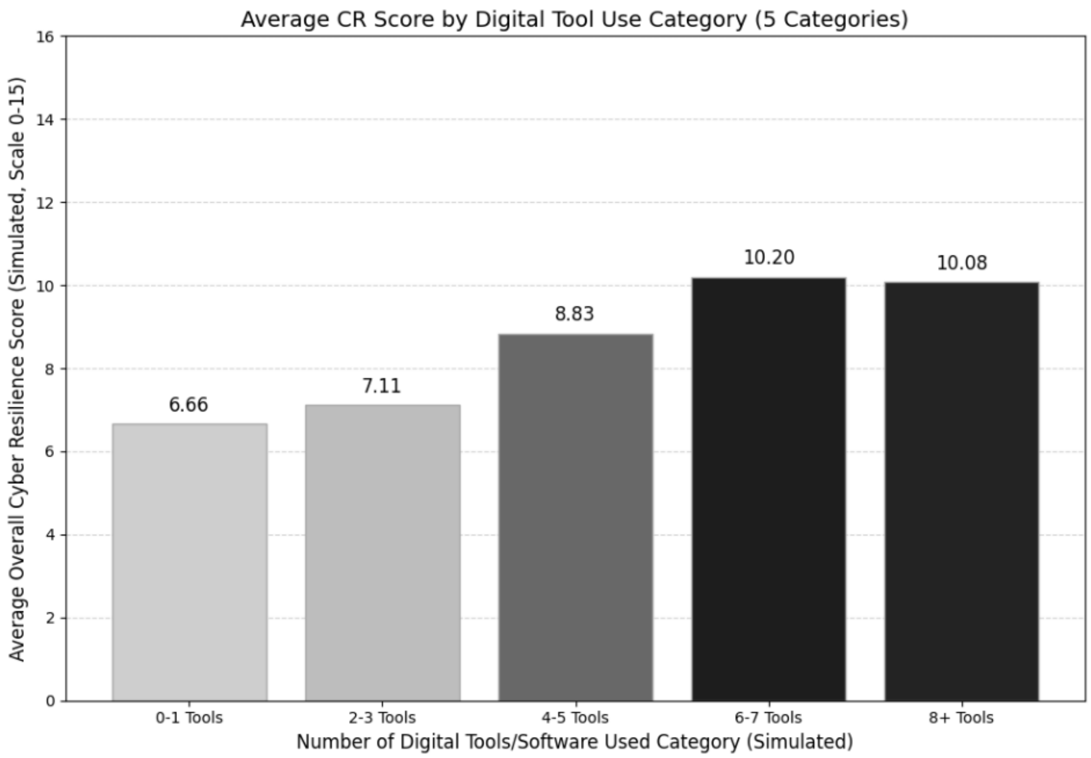


Figure 4.10 Average Cyber Resilience Score by Digital Tool Use Category

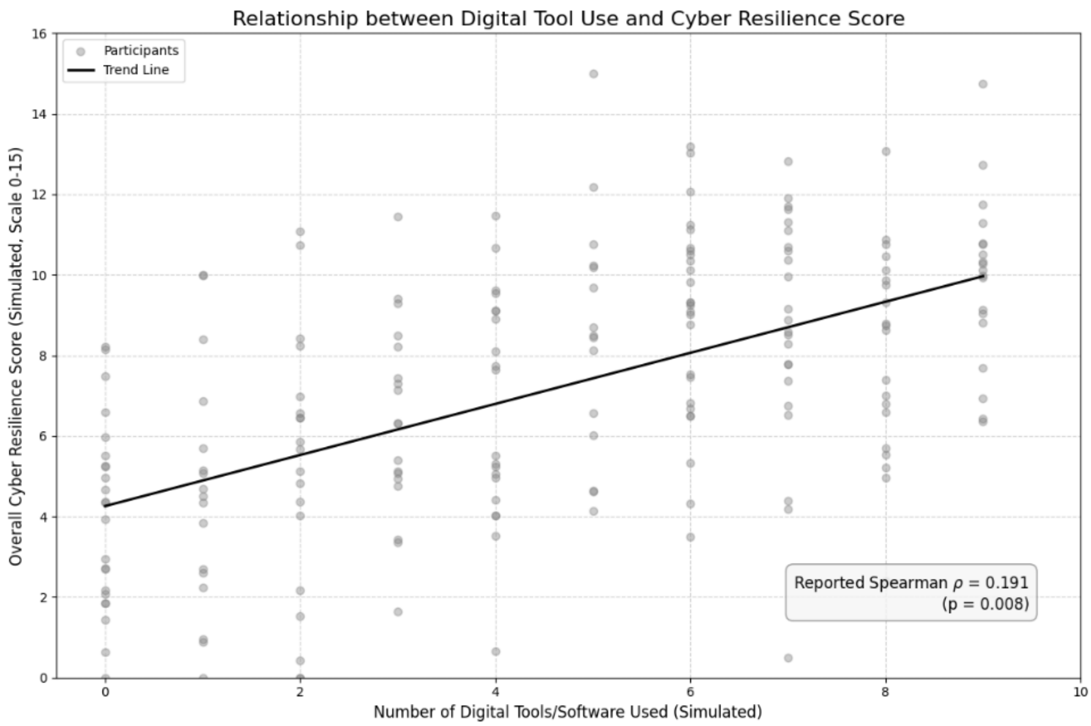


Figure 4.11 Relationship Between Digital Tool Use and Cyber Resilience Score

4.3.2 Correlation with Professional Experience

To investigate the research question, "To what extent do demographic and behavioral variables, gender, digital tool competencies, daily internet use, professional competencies, and whether or not to receive cyber security training affect teachers' cyber resilience levels?", the study examined the relationship between various factors and teachers' cyber resilience. Specifically, Spearman Table 4.6 shows the results of a correlation analysis to determine the direction and level of the relationship between teachers' cyber resilience scores and Professional Experience Years. Therefore, we can see the impact of experiences gained in business life.

Table 4.6 Spearman Correlation Between Teachers' Cyber Resilience and Years of Professional Experience

			Total Cyber Resilience Score	**Years of Experience**
Spearman's rho	**Total Cyber Resilience Score**	Correlation Coefficient	1,000	,003
		Sig. (2-tailed)	.	,970
		N	192	192
	Years of Experience	Correlation Coefficient	,003	1,000
		Sig. (2-tailed)	,970	.
		N	192	192

Table 4.6 and Figure 4.13, shows no significant relationship between teachers' years of professional experience and their overall cyber resilience scores ($\rho = .003$, $p = .970$, $N = 192$). The correlation coefficient obtained is close to zero, implying no significant monotonic relationship between these two variables and between professional experience groups that is shown in the Figure 4.12. As a result, it is concluded that years of professional experience have no bearing on the level of cyber resilience in this study.

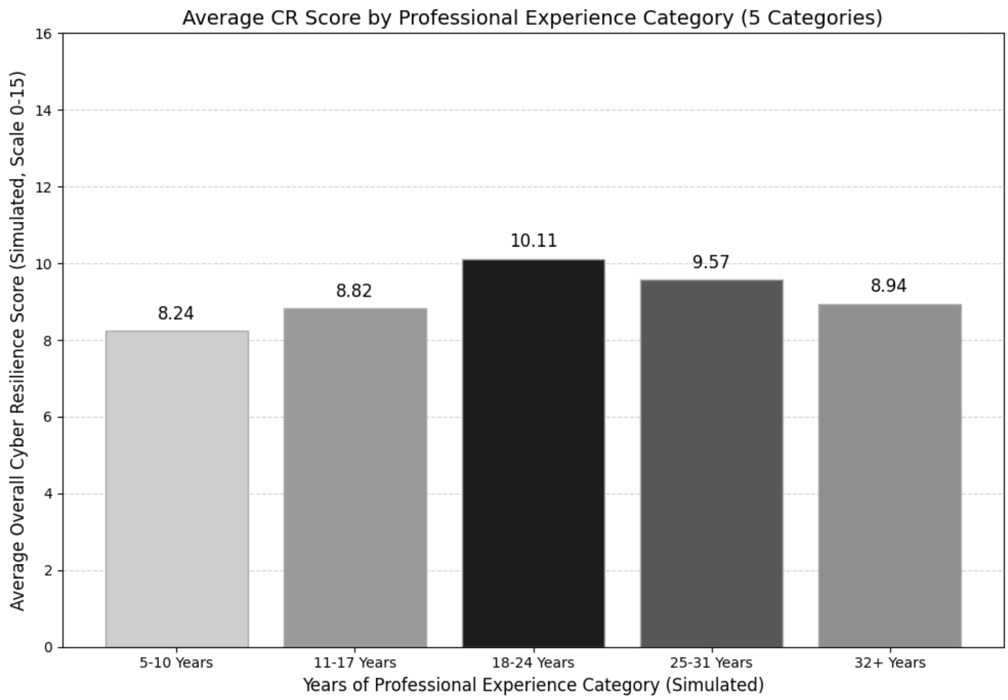


Figure 4.12 Average Cyber Resilience Score by Professional Experience Category

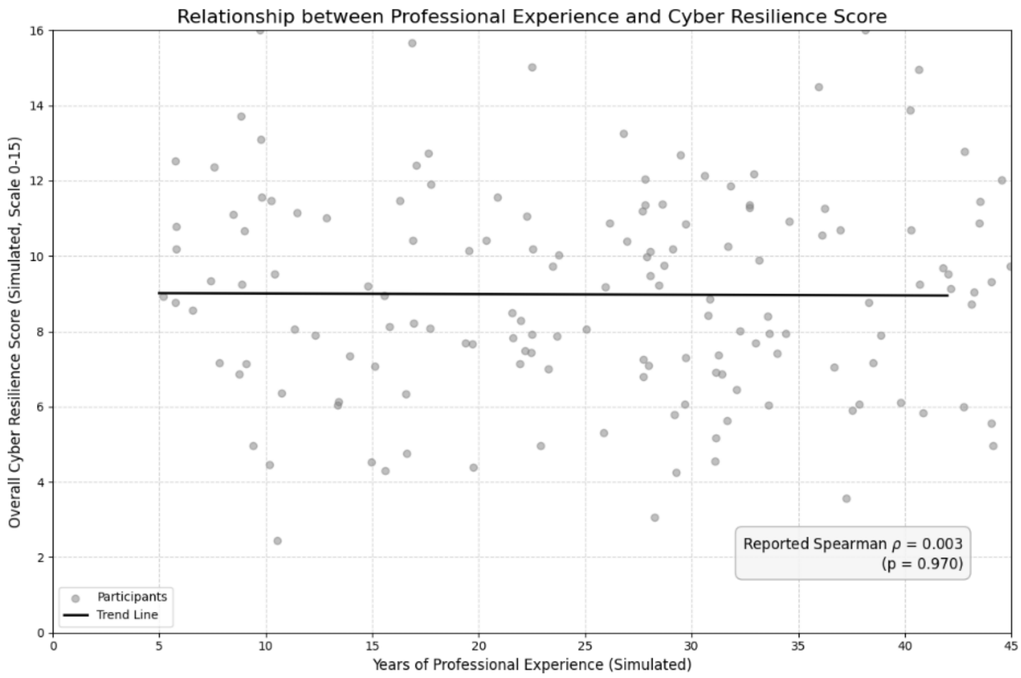


Figure 4.13 Relationship between Professional Experience and Cyber Resilience Score

4.4 Summary of Findings

Based on the central tendency of composite scores, the overall results indicate that teachers have below-average cyber resilience. In addition, there is a variation among cyber resilience abilities based on NIST CSF functions. For example, teachers scored extremely low on the "Detect," "Respond," and "Recover" functions, indicating a weakness in dealing with cyberattacks encountered spontaneously in daily life. However, they were relatively better at the "Protect" function, indicating prevention awareness, such as setting passwords. Moving on, male instructors scored higher than female instructors on cyber resilience measures; therefore, the differences were statistically significant by gender, but both groups performed below average. Furthermore, previous cybersecurity training appeared to be a significant factor; thus, teachers who had received cybersecurity training performed significantly better than teachers who had not received training. Teachers' skills in mastering different digital technologies showed a weak but statistically positive correlation. In contrast, teachers' years of experience or daily internet usage rate did not have a relationship with cyber resilience.

CHAPTER 5

DISCUSSION

This chapter discusses how primary school teachers' cyber resilience is measured and assessed. The U.S National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), which is regarded as a kind of gold standard in the field of cybersecurity, was the instrument selected for this study. The results of the extensive work are presented in this chapter.

5.1 Discussion of Overall Cyber Resilience Levels

The findings of our study, when we look at the median and mean values, reveal that primary school teachers exhibit a moderate level of cyber resilience; in addition, it is closely aligned with previous literature that points to limited awareness and preparedness of these teachers (Guillén-Gámez et al., 2024). This level of resilience is alarming given the frequent target of cyberattacks, the role of teachers, and the sensitive student and institutional data that resides there (Altınöz et al., 2019; Sapanca & Kanbul, 2022; REMS, 2024; Amoroso & Magnan, 2025; Check Point, 2022; Sophos, 2024).

Among the measured cyber resilience sub-dimensions, Protection emerged as the strongest area. Some literature contradicts this result; for example, there remain persistent gaps in advanced protective measures such as password management (Aslanlı & Özdoğru, 2023; Kruger et al., 2010; Yılmaz et al., 2016), data encryption, and multi-factor authentication (Anwar et al., 2024). On the other hand, our findings suggest some general awareness and adoption of basic security practices (Canoğulları, 2021; Varkan Kavas et al., 2022), which is consistent with previous findings that teachers tend to adopt basic protective measures such as the use of antivirus software (Kapanoğlu, 2016; Canoğulları, 2021). However, other important dimensions, such as

Detection and Recovery, scored relatively low, indicating teachers' openness. Low Detection scores reflect teachers' documented difficulties in detecting specific threats such as phishing and other sophisticated cyberattacks (Eroğlu, 2023; Canoğulları, 2021). The particularly low Detection score indicates a fundamental inability to promptly recognize early warning signs or precursor cues of cyberattacks, which is a serious vulnerability that increases the risk of damage escalation (Tazi et al., 2021). Similarly, limited Recovery capabilities indicate skill gaps and insufficient institutional support for incident response and system restoration (Tomczyk, 2024; Anwar et al., 2024; Ravichandran et al., 2025). Again, as highlighted by Altinöz et al. (2019) and Benzer & Karal (2023), these shortcomings are exacerbated by a lack of targeted training and institutional support.

Thus, the overall score reinforces this pattern. The Intervention and Identification dimensions are slightly above average, but Detection and Remediation are low, indicating inconsistent competencies between the resilience aspects. While these five functions should support each other and increase in parallel, they show an inconsistent distribution. In addition, the non-normal distribution indicates heterogeneity in teachers' cyber resilience. This is likely to reflect different levels of education, experience, and resource availability. Mixed scores support the broader literature emphasizing the "human factor" as a critical vulnerability in cybersecurity in the educational context (IBM Corp, 2015; Colwill, 2010).

Overall, the observed moderate cyber resilience underscores the urgent need for comprehensive capacity-building initiatives tailored to the specific skills gaps identified, particularly in threat detection and incident recovery. Developing teacher training programs to address these weaknesses will be vital to strengthening the education sector's cybersecurity posture and mitigating the potentially severe consequences of cyber incidents.

Overall, the moderate cyber resilience observed underscores an urgent need for comprehensive capacity-building initiatives tailored to the specific skill deficits identified, particularly in threat detection and incident recovery. Enhancing teacher training programs to address these weaknesses will be vital to strengthen the education sector’s cybersecurity posture and mitigate the potentially severe consequences of cyber incidents.

5.2 Discussion of Factors Influencing Cyber Resilience

This chapter explains how primary school teachers' cyber resilience is measured and assessed. The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), widely regarded as a gold standard in cybersecurity, was chosen as the study's instrument. Despite some preliminary research on NIST CSF's functions related to educators, no comprehensive effort has been made to determine whether instructors are functionally robust regarding cyber risks. This chapter presents the findings from extensive research.

5.2.1 The Role of Gender

According to the findings, there is a statistically significant difference in cyber resilience scores between male and female primary school teachers. Except for the Responsiveness function, men performed better than women in the total score and NIST Cybersecurity Framework (CSF) functions. The Mann-Whitney U test results and the median scores also show this situation. This situation is consistent with studies in the literature reporting that men have higher cybersecurity awareness and prevention skills than women. For example, Sapanca and Kanbul (2022) found that male teachers in Türkiye exhibited higher information security awareness. Similarly, Guillén-Gámez et al. (2024) reported that male teachers in Spain had stronger cybersecurity skills. Again, Al-Habashneh (2023) observed higher cybersecurity awareness in male teachers in Jordan. To explain this, we can again look at the research conducted by Kabataş Memiş (2023). According to the study, male teacher candidates achieved higher digital fluency scores. Thus, digital fluency may reflect gender differences in technology use or risk perception.

However, the gender-cyber resilience relationship is complex and not universally consistent. Some meta-analyses and studies conducted in Türkiye have found weak or no differences between genders (Arı & Çarkıt, 2020; Çelik & Kaya, 2019). Furthermore, studies on cyberbullying sensitivity and experiences among teachers have found no gender differences (Çelik & Kaya, 2019). These mixed results suggest that factors beyond gender, such as professional experience, quality and quantity of cybersecurity training, digital competencies, and socio-cultural influences, may play critical roles in cyber resilience.

Some studies have shown that resilience manifests itself differently between genders. Accordingly, it implies that interventions aimed at increasing resilience, including cyber resilience, can benefit from gender-sensitive approaches (Bawadi et al., 2022; Stuart, 2025). Based on these, it should be considered that both male and female educators have moderate levels of cyber resilience. Therefore, cybersecurity training should be provided to both groups regardless of gender. Moreover, considering that teachers are generally women, such training should be provided in all forms. Cyber resilience training programs should be inclusive and adapted to address specific needs and gaps identified among all educators. Therefore, future research is needed to investigate the underlying causes of the observed gender inequalities, including psychological, social, and educational factors, and to examine how these dynamics interact with other variables such as age, experience, and institutional support. Nevertheless, the verbal parts of the data should be investigated through a qualitative study before converting them to numerical form.

5.2.2 The Critical Role of Cybersecurity Training

The findings revealed a substantial, statistically significant difference in cyber resilience scores between teachers who received and did not receive cybersecurity training. In other words, teachers who reported receiving cybersecurity training had higher cybersecurity scores than their untrained colleagues. Therefore, training is crucial in equipping primary school teachers with the necessary knowledge and skills to deal with cyber risks effectively.

This result is consistent with the growing literature emphasizing the importance of cybersecurity awareness and training programs in increasing cyber resilience (Akor et al., 2024; Ravichandran et al., 2025; Sağlam et al., 2023). When considered together with the results of other research questions, the most essential factor, training, shows that cyber resilience is not a passive skill acquired through experience or exposure to technology; on the contrary, it is an active competence developed through targeted training and professional development.

Aside from these, in Türkiye, many studies emphasize significant deficiencies in teacher training related to cybersecurity and digital literacy. For example, Altınöz et al. (2019) reported that many teachers felt inadequate in cybersecurity. Güleç and Noyan (2024) emphasized the complex relationship between technology adoption and teacher education, thus drawing attention to the need for continuous self-improvement to adapt to digitalization. In another study, Benzer and Karal (2023) revealed that the cybersecurity awareness of IT pre-service teachers who received training was significantly higher than that of their peers. In addition, the difficulties faced by Turkish teachers during the COVID-19 pandemic were revealed in the research, as many of them had trouble with technology use and preparation for online education, further demonstrating the urgent need for improved education (Bavli & Kortel, 2023; Adıgüzel et al., 2024).

Furthermore, international studies emphasize that continuous cybersecurity education is necessary to raise awareness about common threats such as phishing and social engineering (Student Privacy, 2024; REMS, 2024; Amoroso & Magnan, 2025). One study showed that workshops and professional development programs focused on recognizing cyber threats, securing personal devices, and encouraging strong password practices effectively improved teachers' ability to create safer online environments for students (CFISA, 2023). Additionally, embedding cybersecurity awareness in school culture is critical to encouraging a proactive rather than reactive approach to cyber threats (CFISA, 2023; Qawasmeh et al., 2024). Despite this, cybersecurity education is underutilized in many educational settings worldwide, resulting in teachers' lack of skills to detect, respond to, and recover from cyber incidents (Anwar et al., 2024;

Tomczyk, 2024). These studies highlight the need for accessible, high-quality educational resources, including workshops, online training, and peer support networks, to enhance teachers' cybersecurity competencies (Adıgüzel et al., 2024). Some studies show that technology-based solutions alone are insufficient and that developing a strong security culture through education and awareness is crucial (Eminağaoğlu et al., 2010; Glaspie & Karwowski, 2018). Apart from these, changes in the status and quality of education worldwide indicate serious challenges to comprehensively increase teachers' cyber resilience (Ravichandran, Singh, & Sasikala, 2025). In conclusion, the findings of this study confirm that cybersecurity education is an essential determinant of teachers' cyber resilience. To effectively protect educational environments, stakeholders should prioritize developing and implementing comprehensive, ongoing training programs tailored to educators' needs, thus empowering them to navigate the complex and evolving cyber threat landscape safely.

5.2.3 The Role of Digital Tool Usage

According to the findings, a weak, statistically significant positive correlation was found between the amount of digital tools used by primary school teachers and their cyber resilience scores. In other words, educators who use a wider range of digital technology are more cyber-resilient. Therefore, more exposure to various educational digital platforms will help users adopt cyber awareness skills and may increase awareness of cybersecurity risks. However, the weakness of this relationship shows that simply increasing the amount of technology used does not significantly increase cyber resilience. Instead, the quality of technology use- how effectively and consciously one interacts with digital tools- is essential. This finding is consistent with the study of Corradini and Nardelli (2025); for example, this study associates digital self-confidence with ICT use. This situation is particularly striking in the context of the Turkish education system. Studies have documented that although teachers actively produce and store information in digital environments (Çetinkaya et al., 2017), many use the Internet unconsciously and without sufficient cyber resilience

(Karagözlü, 2020). Effective and efficient use of digital technologies emerges as a core competency that can indirectly affect cyber resilience (Özer, 2022). Kabataş Memiş's (2023) study of prospective teachers reveals gender-based differences in digital tool use. Male candidates score higher than females because they use technological tools more frequently.

Additionally, research shows that younger or less experienced teachers tend to have higher ICT competencies and self-efficacy (Durak & Seferoğlu, 2017; Demirer & Sak, 2015), suggesting that age and experience modulate digital tool use and, potentially, cyber resilience. Despite the increasing use of technology in education, challenges persist. Turkish educators have reported technical and instructional challenges related to digital tools and distance education applications that indirectly affect the security environment (Bayrak, Sandıkçı, & Şahin, 2023; Düzgün, 2021). Infrastructure deficiencies and a lack of clear policies make safe technology use even more difficult (Yilmaz & Karadag, 2023). These findings underline that technology adoption alone is insufficient without comprehensive support systems, training, and policy frameworks. Again, Noyan and Güleç (2024) also emphasize the complex relationship between technology adoption and teacher education. This study underlines the need for continuous professional development to adapt to digitalization effectively. The COVID-19 pandemic has revealed deficiencies in teachers' preparedness for online education and related security risks (Bavli & Kortel, 2023; Adıgüzel et al., 2024). On the other hand, the weak relationship reveals that effective cyber resilience encompasses technical competencies and safe and responsible behaviors such as critically evaluating online information, understanding digital footprints, securing data access, and detecting suspicious activities (Tomczyk et al., 2024). Therefore, it is essential to develop teachers' security-related digital tool competencies through targeted workshops, online training, and peer support networks (Adıgüzel et al., 2024).

In summary, although increased use of digital tools is weakly associated with better cyber resilience, this relationship is fundamental and mediated by factors such as digital competence, quality of education, and institutional support. Nevertheless, when it is assumed that the amount of educational digital tool use required from teachers is needed, it is obvious that quality rather than quantity is important here. Therefore, while teachers are provided with digital tool use competencies, supporting this with cyber resilience training will make essential contributions.

5.2.4 The Role of Internet Usage Duration

The findings of this study show that the time teachers spend on the internet daily does not affect their cyber resilience scores. The Kruskal-Wallis H test results showed no statistically significant difference in cyber resilience among the three groups categorized according to daily internet use time. Median tests also confirmed that there were no significant differences between these groups. This shows that the amount of time spent on the internet is independent of the quality of online activities and the extent of basic cybersecurity training and awareness. In addition, this aligns with previous research emphasizing that individuals' cyber risk perceptions, coping strategies, and security practices are more determinant of cyber resilience than exposure or frequency of internet use alone (Chou & Chou, 2016). In another study, Karagözlü (2020) found that trainee teachers often use the internet unconsciously and without sufficient cyber resilience; therefore, they emphasized that habitual internet use does not mean preparedness. Similarly, Sapanca and Kanbul (2022) reported that resilience was not associated with internet use, supporting the idea that exposure alone does not develop sufficient cybersecurity competencies.

Reflecting our data, in the educational context in Türkiye, it is reported that most teachers use the internet for one to three hours per day, while fewer use it for extended periods (Özker, 2022). Accordingly, the literature generally indicates that teachers' cyber awareness and knowledge are lacking. Some studies have found significant relationships between the frequency of internet use and specific online risks such as online bullying (Sezer et al., 2015) or student cybersecurity (Ahmed et al., 2021). However, these findings do not fully reflect cyber resilience.

Aside from these, a study conducted among parents in Türkiye revealed a negative correlation between problematic internet use and happiness and psychological resilience (Gökmen et al., 2023). In other words, excessive or uncontrolled internet use in adults may harm psychological well-being and resilience. Similarly, studies on university students and parents have shown that excessive use can impair focus and awareness, potentially weakening cybersecurity skills (Gökmen et al., 2023; Satıcı, 2019). These findings support the idea that increased internet time decreases rather than increases cyber resilience.

Aside from these, the group of four hours and above, with the fewest people, has the highest score among our three groups. The fact that such a low-numbered group received a high score may suggest that qualitative data should be examined in more detail or that more detailed research should be conducted.

Therefore, when these situations are taken together, cyber resilience is not a function of the duration of internet exposure. Instead, it depends on how individuals interact with digital environments and acquire cybersecurity knowledge and skills. In other words, the quality of technology used is more important for teachers than the quantity.

5.2.5 The Role of Professional Experience

The results revealed no significant correlation between teachers' years of professional experience and cyber resilience scores. It shows that teaching experience does not translate into cyber resilience. This finding is noteworthy because it shows that cyber resilience is not an innate skill or a passive competency developed over the years in the profession. In other words, time spent teaching does not impart the specific knowledge and skills needed to navigate the evolving cyber threat landscape. As a result, targeted training and deliberate skill development are essential to fostering cyber resilience.

This is consistent with previous research showing that while professional experience benefits many aspects of teaching, it does not inherently enhance competencies such as IT self-efficacy or cyber resilience (Corradini & Nardelli, 2025). Similarly, Yılmaz, Şahin, and Akbulut (2016) found no statistically significant difference in teachers' digital data security awareness based on their professional experience; the results of this study reinforce the need for formal cybersecurity training regardless of tenure.

Studies show cybersecurity awareness decreases with age (Canoğulları, 2021; Yayla, 2018). Older teachers, who usually encounter technology later in their careers, may not be familiar with digital security measures. In support of this, Durak and Seferoğlu (2017) and Sak and Demirer (2015) reported that younger or less experienced teachers exhibited higher competence and self-efficacy in information technologies. This disparity is likely related to the earlier exposure of young educators to technology because young people are more adapted to the information society and have a more developed understanding of digital citizenship (Canoğulları, 2021).

However, the lack of a relationship between years of teaching and cyber resilience suggests that factors beyond digital competence, age, and experience, such as training, are essential in shaping resilience against cyber threats (Özker, 2022).

This highlights the importance of integrating comprehensive cybersecurity training and continuing professional development into teacher preparation programs and seminar sessions to address current deficiencies. In summary, the findings highlight that cyber resilience is a distinct competency that requires deliberate development through specialized training rather than passive acquisition through professional experience. Addressing this need is crucial to preparing educators to effectively protect digital environments and respond to emerging cyber risks in education.

5.3 Implications of the Findings

The findings contribute to a theoretical understanding of teachers' cyber resilience in professional situations. This section addresses these issues and offers suggestions for improving educational institution security. The goal is to protect schools from cyber threats, which are becoming more prevalent with the increased use of digital technology. As a result, gaps in the field should be filled, and factors that promote resilience will be explored.

5.3.1 Theoretical Implications

This study measures the reducibility of the NIST Cybersecurity Framework (CSF), a cybersecurity framework primarily preferred by institutions for embedding in systems, to the individual. This study tested the NIST Cybersecurity Framework (CSF), a cybersecurity framework primarily preferred by institutions for embedding in systems, by translating it to the individual and education sectors. The alignment of the findings with the literature created the possibility that cybersecurity frameworks could be used as a tool that can be effectively adapted to assess and determine individual teacher competencies in cyber resilience (Alshar'e, 2023). In other words, this adaptation demonstrates the possibility of meaningfully translating cyber competencies traditionally conceptualized at the institutional level to the individual level. In this way, a CSF provides a detailed understanding of educators' strengths and weaknesses. In this research, while teachers exhibit relatively strong protection mechanisms in their use of technology, significant deficiencies were observed in other critical dimensions of cyber resilience, such as detection, intervention, and recovery. The literature also shows that teachers are resilient in issues such as antivirus or secure passwords but weak in detection and response (Tomczyk, 2024; Anwar et al., 2024; Eroğlu, 2023). Accordingly, this scope should be developed for solid cyber resilience to take cybersecurity measures and develop proactive and reactive behaviors.

In addition, it was found that cyber resilience does not naturally emerge through professional experience or long-term exposure to technology. General technology use indicators, such as internet usage time, did not significantly affect resilience levels, reinforcing that cyber resilience is not an innate trait or a byproduct of general professional development (Yılmaz et al., 2016; Sapanca & Kanbul, 2022). This study found that formal education and training emerged as the only significant positive predictor of cyber resilience among the variables examined. These results support theoretical models that emphasize the interplay of knowledge acquisition, skill development, and ongoing learning in shaping cybersecurity behavior and capacity (Akor et al., 2024; Ravichandran et al., 2025).

In short, cyber resilience is a competency developed through individual-level training. As a result, future theoretical studies should focus on creating refined models specific to teachers that build knowledge, skills, and learning pathways to develop effective cyber resilience. Such models will provide a solid foundation for designing evidence-based educational programs and policies that aim to strengthen the cybersecurity posture of educators and schools.

5.3.2 Practical Implications for Teacher Training and School Policy

The study highlights significant deficiencies in the NIST Cybersecurity Framework (CSF) in functions other than protection. While teachers demonstrate proficiency in basic preventive measures such as password management and antivirus use, their abilities in the more complex and dynamic areas of Detection, Response, and Recovery are alarmingly weak. In other words, educators lack the necessary technical skills to recognize early indicators of cyber incidents, initiate appropriate response actions, navigate incident reporting protocols, and execute data recovery procedures. This reflects a deficiency in educational programs (Ravichandran et al., 2025; Tomczyk, 2024).

To bridge this gap, active, experiential learning methodologies should replace traditional passive learning approaches. A controlled environment should be created to assess and develop teachers' practical response skills. Scenario-based exercises, simulations, and real-time drills should be conducted (CFISA, 2023). As the literature suggests, these practical strategies should be integrated into pre-service and in-service teacher education programs. These strategies encourage teacher development and equip them to effectively anticipate and manage cyber incidents (Tazi et al., 2021).

Cybersecurity education should be a mandatory and ongoing component of professional development. There should be single training and regular refresher courses to keep up with the rapidly changing threat landscape (Qawasmeh et al., 2024; Mouwers-Singh & Musikavanhu, 2024). Strengthening school-level policies and infrastructure is equally important. The study revealed teachers' severe lack of awareness about current cybersecurity policies. This indicated gaps in communication and implementation in terms of cybersecurity (Glaspie & Karwowski, 2018). In this case, school administrators should prioritize creating and disseminating transparent, accessible, and enforceable cybersecurity policies and incident response protocols.

However, policies alone are not enough. Effective communication strategies are essential for educators to take responsibility and action during cyber emergencies. Regular training sessions, accessible documentation, and hands-on workshops can reinforce this understanding. In addition, IT staff should routinely review and update these protocols to communicate emerging threats and technological advances (Verizon Business, 2023). Additionally, they should ensure that the school's cybersecurity posture remains agile and resilient.

School leadership is critical in fostering a culture of shared responsibility for cybersecurity (Colwill, 2010; Eminağaoğlu et al., 2010). Administrators should support the integration of cybersecurity into the school's core values and encourage awareness and accountability at all levels. In other words, it requires specific budgets for comprehensive educational programs, investments in secure technology infrastructure, and user-friendly technical support for educators.

Empowering teachers through training and resources increases their resilience and fosters awareness, strengthening the school's cybersecurity framework. According to the literature, when educators feel supported and empowered in cybersecurity, they are more likely to contribute to protecting student data and ensuring continuity of instruction; in addition, they are more likely to actively contribute to reducing cyber risks (Tazi et al., 2021).

In addition to these measures, schools should consider establishing cross-functional cybersecurity committees that include teachers, IT staff, and administrators. Such collaborative bodies can support effective communication and identify emerging threats, coordinate response efforts, and provide a proactive and unified approach to cybersecurity (Fouad, 2021).

Finally, partnerships can be established with external cybersecurity experts and organizations. This can provide valuable insights, resources, and training opportunities, further strengthening schools’ ability to defend against cyber threats (Ronen, 2024). Schools can create resilient environments where educators and students are protected in the digital age by adopting a holistic, multi-layered strategy that integrates education, policy, culture, and collaboration.

CHAPTER 6

CONCLUSION

The final chapter summarizes the main findings from the study on primary school teachers' cyber resilience. Which is the summary, conclusions, limitations, recommendations for future research and recommendations for practice.

6.1 Summary of the Study

This study assessed the cyber resilience of primary school teachers using the NIST Cybersecurity Framework. The study found that overall, participants' cyber resilience was below the expected level of competence. While educators scored relatively high in implementing basic prevention measures, primarily part of the 'Protect' function in the CSF, gaps were discovered in other equally important areas. Participants' competence in the 'Detect' (threat detection), Respond' (incident response), and 'Recover' (system recovery after incidents) functions were particularly low.

A statistically significant positive relationship was found between teachers' cybersecurity training and cyber resilience scores. No statistically significant relationship was found between the length of professional experience and the number of daily hours spent on the internet and cyber resilience. Furthermore, a weak positive relationship was found between the number of digital tools teachers use and cyber resilience scores. Finally, statistically significant gender differences were discovered, with male teachers scoring higher than female teachers on most CSF dimensions ('Identify,' 'Protect,' 'Detect,' and 'Recover'). However, there was no score difference on the 'Respond' dimension.

6.2 Conclusions

Firstly, it was concluded that the primary school teachers participating in the study were unprepared for daily cybersecurity incidents outside of standard security measures. Teachers were particularly unprepared regarding threat detection, incident response, and recovery in case of security breaches. Secondly, the positive correlation with cyber resilience suggests that appropriate and specific cybersecurity training is an essential and applicable way to increase teachers' preparedness.

Thirdly, there was no relationship between resilience and professional experience. There was also no significant relationship between the duration of internet use. Therefore, it supports the idea that cyber resilience is not a by-product of teaching experience or technology use. Thus, cyber resilience should be developed through specific practices and awareness-raising activities. Fourthly, the fact that there was a minimal relationship between the amount of digital tools used and resilience indicates that simply introducing more technology into the classroom is not enough to develop cyber resilience. In other words, it shows that security-conscious and careful use should be included in the process.

Finally, despite gender differences, both groups must improve resilience scores. All educators should receive professional training to become cyber-resilient. The current level is still far below the level required to overcome the challenges of ensuring continuity and protecting sensitive data in increasingly digital educational environments.

6.3 Limitations of the Study

The study sample was limited to primary school teachers working in public schools in the Ankara region. Due to this population restriction, the findings may not apply to teachers in other settings, such as schools in other regions of Türkiye or private schools, or to educators in other positions, such as subject matter experts or school administrators. Second, the data are based mainly on self-reported data through survey measures. Self-reported information is somewhat compromised because the participants' statements were evaluated objectively. In other words, the answers given may reflect their perceived competence rather than their competence. Therefore, it may lead to over- or underestimation of the actual implementation levels of cyber resilience and cyber resilience itself.

6.4 Recommendations for Future Research

Expanding the study frame to include teachers from other regions, public and private school teachers, and school administrators is an important step. Including more diverse participant groups, such as different age groups and positions, will increase the representativeness and generalizability of the findings of future studies. Methodologically, future studies can benefit from mixed-method research. Surveys can be conducted with qualitative data, such as interviews and focus groups; they can be combined with performance measures (such as scenario tests and technical tests). In this case, it will provide more complete and objective information about teacher resilience in a broader sense. The deeper reasons for the gender differences observed in cyber resilience scores should be revealed. In addition, more research is needed to investigate the effects of digital literacy cybersecurity training experiences. In other words, examining the long-term impact and effectiveness of various cybersecurity training and studies more rigorously would be helpful. Investigating or even simulating employees' daily experiences and risk perception is necessary. In other words, monitoring cyber resilience over a while would be helpful. Investigating the relationships between school variables, namely school policy, available resources and IT support, and teacher resilience, would also make significant contributions.

6.5 Recommendations for Practice

One of the main recommendations is to create and implement specific professional development interventions for all school personnel. These should address the NIST CSF functions of ‘Detect,’ Respond,’ and ‘Recover’ vulnerabilities. The training provided should be a combination of theory and scenario practice to develop usable skills. Consideration should be given to making the training ongoing and mandatory to ensure competency. Second, cybersecurity policies in schools should be developed comprehensively and with discipline; in addition, they should be rigorously implemented. These policies should be communicated to all school personnel and successfully implemented.

Furthermore, there should be a way to validate and update the policies as needed. Third, cybersecurity and cyber resilience training should be included as a mandatory component in the pre-service education curriculum. This will ensure that new teachers start their careers with a solid foundation of knowledge and preparation. Finally, ensuring that teachers protect themselves, their students, and institutionally confidential information in an ever-digital environment is not just a suggestion. It is a call to action. The findings highlight the importance of accelerating systematic and focused interventions such as special education, concrete policy, and curriculum integration to create a healthy culture of cyber resilience among teachers.

REFERENCES

Adıgüzel, T., Kaya, M. F., & Ersoy, A. (2024). Digital Competence of Educators in Türkiye According to European Digital Competence Framework. Journal of Learning and Teaching in Digital Age, 9(1), 97–108.

Ahmed, O. S., Nasef, S. A., Al Rawashdeh, A. Z., & Eltahir, M. E. (2021). Teacher's awareness to develop student cyber security: A Case Study. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 5148–5156.

Akor, S. O., Nongo, C., Udofot, C., & Oladokun, B. D. (2024). Cybersecurity awareness: Leveraging emerging technologies in the security and management of libraries in higher education institutions. Southern African Journal of Security. https://doi.org/10.25159/3005-4222/16671

Al-Habashneh, A. A. (2023). The Degree of Cyber Security Awareness among Teachers in the Karak Education Directorate. Zarqa University Journal for Research in Humanities, 23(3), 662–679.

Al-Hawamleh, A. (2024). Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security. International Journal of Computing and Digital Systems, 15(1), 1315-1331. https://doi.org/10.12785/ijcds/150193

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432-445. https://doi.org/10.1016/j.cose.2009.12.005

Alshar'e, M. (2023). Cyber security framework selection: Comparison of NIST and ISO27001. Applied Computing Journal, [Volume/Issue information missing], 245–255. https://doi.org/10.52098/acj.202364

Altınöz, M., Tosun, N., Çinkılıç, T., & Çay, E. (2019). Siber güvenlik ve bilinçli sosyal medya kullanımı dersi pilot uygulamasına ilişkin öğretmen görüşleri [Teacher views on the pilot application of the cybersecurity and conscious social media use course]. Journal of Continuous Vocational Education and Training, 2(1), 1–15.

Alwahaibi, A., Bin, W. H. W., Hassa, W. N. W., Basri, S. W., Wan Ismail, W. B., & Almamari, M. (2022). A systematic literature review on IT security standards for higher education institution. Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/Journal of Tianjin University Science and Technology, 55, 194-213.

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security, 12, 233-249. https://doi.org/10.4236/jis.2021.124013

Amoroso, L. M., & Magnan, M. (2025). Cybersecurity in education: Protecting students and staff [Manuscript]. ResearchGate. https://www.researchgate.net/publication/388458382_Cybersecurity_in_Education_Protecting_Students_and_Staff

Anwar, N., Juanda, Anderson, J., & Williams, T. (2024). Applying data science to analyze and improve student learning outcomes in educational environments. International Transactions on Education Technology (ITEE), 3(1), 72–83. https://doi.org/10.33050/itee.v3i1.679

Arı, F., & Çarkıt, Y. (2020). Investigation of Resilience in Terms of Gender: A Meta-Analysis Study. Research on Education and Psychology, 2(1), 37–41.

Aslanlı, M., & Özdoğru, M. (2023). Okul yönetiminde dijital veri güvenliği: Tehditler ve önlemler [Digital data security in school administration: Threats and precautions]. Anadolu Eğitim Liderliği Ve Öğretim Dergisi, 11(1), 48-66.

Ayyildiz, P., Yilmaz, A., & Baltaci, H. S. (2021). Exploring digital literacy levels and technology integration competence of turkish academics. International

Journal of Educational Methodology, 7(1), 15-31. https://doi.org/10.12973/ijem.7.1.15

Bandura, A. (1994).. Self-efficacy. In V. S. Ramachaudran (Ed.), Encyclopedia of human behavior (Vol. 4, pp. 71–81). Academic Press.

Bavli, B., & Kortel, Ö. (2023). Teacher Resilience in the Face of Uncertainty: Experiences of Turkish Teachers during the COVID-19 Outbreak. Pastoral Care in Education, 41(3), 346–368.

Bawadi, M. A., Abu-Shanab, S., Al-Twalbeh, M. A., & Alomari, M. K. (2022).. Gender Differences in Coping Strategies and Resilience among Syrian Refugees in Jordan. Journal of International Migration and Integration, 23(4), 1789–1807.

Bayrak, Ö., Sandıkçı, F., & Şahin, T. G. (2023). Turkish Teachers' Experiences on the Distance Education Process and Technological Education Tools. Malaysian Online Journal of Educational Technology, 11(4), 226-237.

Benzer, A. I., & Karal, Y. (2023). Pre-service teachers' information security awareness: An analysis based on the knowledge-attitude-behavior model. Educational Academic Research, (49), 10-22. https://doi.org/10.5152/AUJKKEF.2023.1034562

Bıçakcı, S., & Gücüyener Evren, A. (2025).. Sihirli Reçete mi, Kara Kutu mu: Siber Krizlere Karşı Esnek-Dayanıklılık Anlatısının İncelenmesi [Magic Recipe or Black Box: Examining the Narrative of Cyber Crisis Resilience]. REFLEKTİF Sosyal Bilimler Dergisi, 6(1), 59–80. https://doi.org/10.47613/reflektif.2025.202

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In Advances in Intelligent Systems and Computing (Vol. 353, pp. 311-316). Springer, Cham. https://doi.org/10.1007/978-3-319-16486-1_31

Bouke, M. A., Abdullah, A., Hamoud, S., Zaid, S., & El Atigh, H. (2023). The intersection of targeted advertising and security: Unraveling the mystery of overheard conversations. Telematics and Informatics Reports, 11, 100092.

Brown, L. (2023). Digital citizenship: A journey to internet safety (Master's thesis, Illinois State University). Illinois State University Theses and Dissertations. https://doi.org/10.30707/ETD2023.20230711063200807142.999994

Canoğulları, E. (2021). Öğretmenlerin bilgi güvenliği konusundaki farkındalıklarının incelenmesi [Investigation of teachers' awareness of information security]. Kalem Eğitim ve İnsan Bilimleri Dergisi, 11(2), 651–679. https://doi.org/10.23863/kalem.2021.219

Carvalho, S., Carvalho, J., Silva, J., Santos, G., & Bandeira, G. (2023). Concerns about cybersecurity: The implications of the use of ICT for citizens and companies. Journal of Information Systems Engineering and Management, 8(4), 20713. https://doi.org/10.55267/iadt.07.13226

Center for Information Security Awareness. (2023). How to improve cybersecurity awareness in educational institutions. https://www.cfisa.com/how-to-improve-cybersecurity-awareness-in-educational-institutions/

Çelik, S., & Kaya, N. (2019). The Analysis of Teachers' Cyber Bullying, Cyber Victimization and Cyber Bullying Sensitivity Based On Various Variables. Eurasian Journal of Educational Research, 8(4), 1029–1038.

Çetinkaya, E., Güldüren, Y., & Keser, H. F. (2017). Öğretmenlerin bilgi güvenliği konusundaki farkındalıkları [Teachers' awareness of information security]. Kalem Eğitim ve İnsan Bilimleri Dergisi, 7(1), 1-24.

Çetinkaya, E., Güldüren, Y., & Keser, H. F. (2021). Öğretmenlerin dijital veri güvenliği farkındalıklarının incelenmesi [Investigation of teachers' digital data security awareness]. SUJE, 6(2), 101-114. https://dergipark.org.tr/en/pub/suje/article/261095

Check Point Software Technologies Ltd. (2022). Cyber security report 2022. https://www.checkpoint.com/cyber-security-report-2022/

Chou, H.-L., & Chou, C. (2016). An Analysis of Multiple Factors Relating to Teachers' Problematic Information Security Behavior. Computers in Human Behavior, 65, 334–345. https://doi.org/10.1016/j.chb.2016.08.034

Clever. (2023, January 5). New survey: 1 in 4 schools were victims of cyberattacks in the last year; administrators to increase spending on privacy and security. PR Newswire. https://www.prnewswire.com/news-releases/new-survey-1-in-4-schools-were-victims-of-cyberattacks-in-the-last-year-administrators-to-increase-spending-on-privacy-and-security-301713829.html

Cohen, J. (1960). A coefficient of agreement for nominal scales. Educational and Psychological Measurement, 20(1), 37–46. https://doi.org/10.1177/001316446002000104

Colwill, C. (2010). Human Factors in Information Security: The Insider Threat-Who Can You Trust These Days? Information Security Technical Report, 14(4), 186-196. https://doi.org/10.1016/j.istr.2010.04.004

Corradini, I., & Nardelli, E. (2025). Insights into Teachers' Self-efficacy in Informatics Education. The Educational Review, USA, 9(1), 1-9. https://doi.org/10.26855/er.2025.01.001

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage.

Cybersecurity and Infrastructure Security Agency. (2020). Cybersecurity and Infrastructure Security Agency (CISA). USAGov. https://www.usa.gov/agencies/cybersecurity-and-infrastructure-security-agency

Cybersecurity and Infrastructure Security Agency. (2024). If you think you've been hacked. https://www.cisa.gov/news-events/news/if-you-think-youve-been-hacked

Cybersecurity and Infrastructure Security Agency. (2024). Protect yourself from phishing. https://www.cisa.gov/news-events/news/protect-yourself-phishing

Cybersecurity and Infrastructure Security Agency. (2024). Understanding and using multi-factor authentication. https://www.cisa.gov/news-events/news/understanding-and-using-multi-factor-authentication

Cybersecurity and Infrastructure Security Agency. (2024). Understanding social engineering.

Demirer, V., & Sak, N. (2015). Türkiye'de Bilişim Teknolojileri (Bt) Eğitimi Ve Bt Öğretmenlerin Değişen Rolleri. Uluslararası Eğitim Bilimleri Dergisi(5), 434-448.

Department for Science, Innovation and Technology. (2024, April 9). Cyber Security Breaches Survey 2024. GOV. UK. https://www.gov.uk/official-statistics/cyber-security-breaches-survey-2024

Dunn Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: adding social considerations to technological fixes. Journal of Risk Research, 26(7), 801–814.

Durak, H. Y., & Seferoğlu, S. S. (2017). Öğretmenlerde Tükenmişlik Duygusunun Çeşitli Değişkenler Açısından İncelenmesi. Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi, 37(2), 759-788.

Düzgün, S. (2021). Teachers' Attitudes toward Türkiye Education Informatics Network during the Distance Education Period in the Covid-19 Pandemic. International Journal of Progressive Education, 17(5), 102-118. https://doi.org/10.29329/ijpe.2021.375.8

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2010). The positive outcomes of information security awareness training in companies – A case study. Information Security Technical Report, 14(4), 223-229. https://doi.org/10.1016/j.istr.2010.05.002

Emsisoft Malware Lab. (2023). The state of ransomware in the U. S.: Report and statistics 2022. https://www.emsisoft.com/en/blog/category/malware-lab/ransomware/

Eroğlu, C. (2023). İşletmelerin maruz kaldığı siber suçların boyutu [The extent of cybercrimes faced by businesses]. Güvenlik Bilimleri Dergisi, 12(1), 69-96.

Federal Trade Commission. (2016, August 31). NIST Cybersecurity Framework and the FTC. Retrieved from https://www.ftc.gov/business-guidance/blog/2016/08/nist-cybersecurity-framework-and-ftc

Fitria, H., & Suminah, S. (2020). Role of Teachers in Digital Instructional Era. Journal of Social Work and Science Education, 1(1), 70-77. https://doi.org/10.52690/jswse.v1i1.11

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

Glaspie, H. W., & Karwowski, W. (2018). Human Factors in Information Security Culture: A Literature Review. In D. Nicholson (Ed.), Advances in Intelligent Systems and Computing (Vol. 593). Springer, Cham. https://doi.org/10.1007/978-3-319-60585-2_25

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. Journal of Cybersecurity, 6(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005

Gökmen, F. M., Gökmen, Ö., & Horzum, M. B. (2023). Problematic internet usage of parents: The mediating roles of happiness, psychological resilience, and dispositional hope. Frontiers in Psychiatry, 14, 1109829.

Gu, Q., & Day, C. (2013). Challenges to teacher resilience: Conditions count. British Educational Research Journal, 39(1), 22–44.

Guillén-Gámez, F. D., Martínez-García, I., Alastor, E., & Tomczyk, Ł. (2024). Digital Competences in Cybersecurity of Teachers in Training. Computers in the Schools, 41(3), 281–306. https://doi.org/10.1080/07380569.2024.2361614

Hochwald, I. H., Green, G., Sela, Y., Radomyslsky, Z., Nissanholtz-Gannot, R., & Hochwald, O. (2023). Converting qualitative data into quantitative values using a matched mixed-methods design: A new methodological approach. Journal of Advanced Nursing, 79(11), 4398–4410. https://doi.org/10.1111/jan.15649

IBM. (2015). IBM 2015 Cyber Security Intelligence Index. https://www.ospi.es/export/sites/ospi/documents/IBM_2015_CyberSecurity_Intelligence_Index.pdf

IKON Insights. (2024, September 24). IKON Insights - September 2024. (Vol. 14).

Internet Crime Complaint Center. (2018). 2018 Internet crime report. Federal Bureau of Investigation. https://www.ic3.gov/AnnualReport/Reports/2018_IC3Report.pdf

International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements. ISO.

Javidi, G., & Sheybani, E. (2018). K-12 Cybersecurity Education, Research, and Outreach. 2021 IEEE Frontiers in Education Conference (FIE), 1–5. https://doi.org/10.1109/fie.2018.8659021

Jawaid, S. A. (2023). Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity. International Journal of Data Science and Big Data Analytics, 2(2), 11-17.

Joint Task Force Transformation Initiative (2013). Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST. SP.800- 53r4

Kabataş Memiş, E. (2023). An Examination of Pre-Service Teachers' Digital Citizenship, Digital Wisdom, and Digital Fluency Levels. International Journal of Assessment Tools in Education, 10(1), 1–20.

Kaşıkcı, Ş., Çağıltay, K., Karakuş, T., Kurşun, E., & Ogan, C. (2014). Bilgi teknolojileri okuryazarlığı ve Türkiye [Information technology literacy and Türkiye]. Hacettepe Üniversitesi Eğitim Fakültesi Dergisi, 29(1), 260-270.

Kapanoğlu, B. (2016). Bilişim teknolojileri öğretmenlerinin bilgi güvenliği hakkındaki farkındalık düzeyleri [Information security awareness levels of information technology teachers]. Mersin Üniversitesi Eğitim Fakültesi Dergisi, 12(1), 170-184.

Karagözlü, D. (2020). Determination of cyber security ensuring behaviours of pre-service teachers. Cypriot Journal of Educational Sciences, 15(6), 1698-1706. https://doi.org/10.18844/cjes.v15i6.5327

Khan, M. M. (2023). NIST Cybersecurity Framework. Journal of Scientific and Engineering Research, 10(8), 150-157.

Klein, R. J. T., Nicholls, R. J., & Thomalla, F. (2004). Resilience to natural hazards: How useful is this concept? Global Environmental Change Part B: Environmental Hazards, 5(1), 35–45. https://doi.org/10.1016/j.hazards.2004.02.001

Korukluoğlu, P., Alcı, B., & Rubach, C. (2023). Reliability and validity of the Turkish version of the teachers' basic ICT competence beliefs scale. International Journal of Assessment Tools in Education, 10(1), 29-55. https://doi.org/10.21449/ijate.995005

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. Information Management & Computer Security, 18(5), 316-327.

Kuş, Z., & Mert, H. (2024). Digital Competence of Educators in Türkiye According to European Digital Competence Framework. Journal of Learning and Teaching in Digital Age, 9(1), 102-114. https://doi.org/10.53850/joltida.1301592

Linkov, I., Eisenberg, D. A., Plourde, K., Yatsalo, B., & Kott, A. (2013). Resilience metrics for cyber systems. Environ Syst Decis, 33, 471–476. https://doi.org/10.1007/s10669-013-9485-y

Linkov, I., & Kott, A. (2018). Fundamental concepts of cyber resilience: Introduction and overview. In I. Linkov & A. Kott (Eds.), Cyber resilience of systems and networks (pp. 1-25). Springer, Cham.

Malecki, A. (2018). Cybersecurity in the classroom: Bridging the gap between computer access and online safety (Cyber Security Capstone Research Project Reports, No. 1). Valparaiso University. https://scholar.valpo.edu/cscrpr/1

Mertens, D. M. (2019). Research and Evaluation in Education and Psychology: Integrating Diversity with Quantitative, Qualitative, and Mixed Methods. Sage Publications.

Mouwers-Singh, C., & Musikavanhu, T. B. (2024). A Narrative Review on Enhancing Cybersecurity in Higher Education Institutions: The Role of Continuous Training and Awareness. Expert Journal of Business and Management, 12(2), 67-73.

National Institute of Standards and Technology. (2021). Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems (NIST Special Publication 800-160, Vol. 2, Rev. 1). U. S. Department of Commerce. https://doi.org/10.6028/NIST. SP.800-160v2r1

Noyan, E., & Güleç, H. (2024). Turkish EFL Instructors' Views on Emergency Remote Online Teaching: Challenges, Opportunities and Suggestions. Journal of Current Debates in Social Sciences, 2(2), 158–174. https://doi.org/10.29228/cudes.73582

Nugroho, F. R., Afiana, F. N., & Kuncoro, A. P. (2024). NIST cyber security framework development for website information collection. Jurnal Teknologi

Sistem Informasi Dan Aplikasi, 7(3), 1335–1342. https://doi.org/10.32493/jtsi.v7i3.41541

Office of the Federal Register, National Archives and Records Administration. (2013, February 12). Executive Order 13636-Improving Critical Infrastructure Cybersecurity. Daily Compilation of Presidential Documents, DCPD-201300091.

Organization of American States, & Amazon Web Services. (2019, August 30). OAS and AWS present white paper to strengthen cybersecurity capacity in the Americas through NIST Cybersecurity Framework.

Özker, H. (2022). Digital Resilience of Teachers: A Mixed Methods Study. In International Conference on Technology and Innovation in Learning, Teaching and Education (pp. 1–8).

Özer, M. (2022). Dijital Okuryazarlık Kavramı ve Öğretmenlerin Dijital Okuryazarlık Düzeyleri Üzerine Bir Araştırma [The Concept of Digital Literacy and a Study on Teachers' Digital Literacy Levels]. Sakarya University Journal of Education, 12(1), 1–21.

Pacific Northwest National Laboratory. (2018). Critical Infrastructure Protection. PNNL. https://www.pnnl.gov/explainer-articles/critical-infrastructure-protection

Petruzzelli, E., & Sharma, N. (2019). Closing the gaps in cybersecurity. Chemical Engineering Progress, 115(11), 35-39.

Qawasmeh, S. A.-D., AlQahtani, A. A. S., & Khan, M. K. (2024). Navigating cybersecurity training: A comprehensive review [Preprint]. arXiv. https://arxiv.org/abs/2401.11326

Ravichandran, R., Singh, S., & Sasikala, P. (2025). Exploring school teachers' cyber security awareness, experiences, and practices in the digital age. Journal of Cybersecurity Education, Research and Practice, 2025(1), Article 1. https://doi.org/10.62915/2472-2707.1214

Readiness and Emergency Management for Schools (2024). K-12 cybersecurity guide. https://rems.ed.gov/docs/REMS_K12_CybersecurityGuide.pdf

Richardson, L. C., Lewis, S. M., & Burnette, R. N. (2019). Building Capacity for Cyberbiosecurity Training. Frontiers in Bioengineering and Biotechnology, 7, 112. https://doi.org/10.3389/fbioe.2019.00112

Ronen, T. (2024, October 3). 31 Must-Know Education Cybersecurity Statistics [Blog post]. Varonis Blog. https://www.varonis.com/blog/education-cybersecurity-statistics

Sağlam, R., Miller, V., & Franqueira, V. (2023). A Systematic Literature Review on Cyber Security Education for Children. IEEE Transactions on Education, 66(3), 274–286. https://doi.org/10.1109/TE.2022.3231016

Santhosh, T., & Thiyagu, K. (2024). Development and validation of cyber security competency scale for prospective teachers. Journal of Pedagogical Sociology and Psychology, 6(3), 111-124. https://doi.org/10.33902/jpsp.202428783

Sapanca, H. F., & Kanbul, S. (2022). Risk management in digitalized educational environments: Teachers' information security awareness levels. Frontiers in Psychology, 13, 986561. https://doi.org/10.3389/fpsyg.2022.986561

Satici, S. A. (2019). The relationship between problematic internet use and social-emotional competence in university students: The mediating role of resilience. Addictive Behaviors Reports, 9, 100148. https://doi.org/10.1016/j.abrep.2018.100148

Sezer, B. (2015). Examining Technopedagogical Knowledge Competencies of Teachers in Terms of Some Variables. Procedia - Social and Behavioral Sciences, 174, 208-215. https://doi.org/10.1016/j.sbspro.2015.01.648

Sezer, B., Yilmaz, R., & Yilmaz, E. (2015). Teacher's awareness to develop student cyber security: A Case Study. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 6(3), 466–475.

Shelim, R. (2024). Cybersecurity in education (Master's thesis, Montclair State University). Montclair State University Digital Commons.

Sinclair, V. G., & Wallston, K. A. (2004). The development and psychometric evaluation of the Brief Resilient Coping Scale. Assessment, 11(1), 94–101. https://doi.org/10.1177/1073191103258144

Smith, S. (2023). Towards a scientific definition of cyber resilience. International Conference on Cyber Warfare and Security, 18(1), 379–386. https://doi.org/10.34190/iccws.18.1.960

Sophos. (2024, April). The state of ransomware 2024 [White paper].

Stuart, J. (2025, May 20). Women Peace and Cybersecurity. https://doi.org/10.17605/OSF. IO/H38WZ

Student Privacy, U. S. Department of Education. (2024). Top 10 cybersecurity tips for teachers. U. S. Department of Education. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Top%20 10%20Cybersecurity%20Tips%20for%20Teachers_508_v3.pdf

Şenoğlu, T., & Çoklar, A. N. (2024). Investigation of Studies and Training Activities on Cyberbullying and Cyber Awareness in Türkiye. Participatory Educational Research, 11(H. Ferhan Odabaşı Gift Issue), 114-127. https://doi.org/10.17275/per.24.97.11.6

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards-A Review and Comprehensive Overview. Electronics, 11(14), 2181. https://doi.org/10.3390/electronics11142181

Tazi, F., Shrestha, S., Norton, D., Walsh, K., & Das, S. (2021). Parents, educators, & caregivers cybersecurity & privacy concerns for remote learning during COVID-19. In CHI Greece 2021: Proceedings of the 1st International Conference of the ACM Greek SIGCHI Chapter (pp. 1–5). Association for Computing Machinery. https://doi.org/10.1145/3489410.3489426

Tomczyk, Ł. (2024). The teacher as a target of cyber-aggression and cyber-bullying: Analysis of selected forms of cyber attacks on educators in Poland. In 12th Euro American Conference on Telematics and Information Systems (EATIS 2024). ACM. https://doi.org/10.1145/3685243.3685248

Tomczyk, Ł., Wójcik, M., & Swacha, J. (2024). Teacher Digital and Media Competence in Cyber Security—A Perspective on Individual Resilience to Online Attacks. Education Sciences, 14(1), 83.

Totseva, Y. R. (2024). Cyber security in school – Digital competence framework for citizens and teacher’s attitude. In 2024 12th International Scientific Conference on Computer Science (COMSCI) (pp. 1-4). Sozopol, Bulgaria. https://doi.org/10.1109/COMSCI63166.2024.10778500

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. International Journal of Information Security, 23, 1695–1719. https://doi.org/10.1007/s10207-023-00811-x

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 13(2), 39. https://doi.org/10.3390/fi13020039

Varkan Kavas, Z., Özbudak, S., & Çetkin, E. (2022). Öğretmenlerin siber güvenliklerinin incelenmesi [Investigation of teachers' cybersecurity]. International Social Sciences Studies Journal, 8(106), 4505–4510.

Verizon Business. (2023). 2023 Data Breach Investigations Report.

Wang, L., Mosher, R. L., & Duett, P. (2024). Cyberattacks and cybersecurity in additive manufacturing. In 2024 IEEE SoutheastCon (SoutheastCon) (pp. 1040–1045). IEEE.

White, G. B., & Sjelin, N. (2022). The NIST Cybersecurity Framework. In I. Management Association (Ed.), Research anthology on business aspects of cybersecurity (pp. 39-55). IGI Global. https://doi.org/10.4018/978-1-6684-3698-1.ch003

Wohlfart, O., & Wagner, I. (2023). Teachers' role in digitalizing education: an umbrella review. Educational Technology Research and Development, 71, 339–365. https://doi.org/10.1007/s11423-022-10166-0

World Economic Forum. (2024). Global Cybersecurity Outlook 2024. WEF.

Yan, Z., Xue, Y., & Lou, Y. (2021). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. Computers in Human Behavior, 121, 106791.

Yaman, S., Bal İncebacak, B., & Sarışan Tungaç, A. (2024). Determination of Teacher Qualifications from the Perspective of Stakeholders: Rubric Development Study. Participatory Educational Research, 11(4), 235-249.

Yayla, H. G. (2018). FATİH projesi uygulanan ve uygulanmayan okullardaki öğretmenlerin bilgi güvenliği farkındalığının incelenmesi (Yayın No. 515405) [Master's Thesis, Ankara Üniversitesi]. YÖK Tez Merkezi.

Yousif Yaseen, K. A. (2022). Importance of Cybersecurity in The Higher Education Sector 2022. Asian Journal of Computer Science and Technology , 11(2), 20–24. https://doi.org/10.51983/ajcst-2022.11.2.3448

Yee, K. P., Mahmud, N. H. N., & Alias, N. A. (2020). Self-disclosure on social media among different cultures: A systematic literature review. Computers in Human Behavior, 107, 106270. https://doi.org/10.1016/j.chb.2020.106270

Yıldırım, Ş., & Varol, F. (2013). Bilgi güvenliği konusunda bireysel farkındalık oluşturmaya yönelik öneriler [Suggestions for creating individual awareness about information security]. Uşak Üniversitesi Sosyal Bilimler Dergisi, 6(4), 257-271.

Yilmaz, R. K., & Karadag, N. (2023). Effects of Emergency Distance Education on Teacher Training Process in Türkiye: Instructors' Opinions. Education Sciences, 13(9), 920. https://doi.org/10.3390/educsci13090920

Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2016). Öğretmenlerin Dijital Veri Güvenliği Farkındalığı [Digital data security awareness of teachers]. Sakarya University Journal of Education, 6(2), 26-45. https://doi.org/10.19126/suje.2965

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

APPENDICES

A. Voluntary Attendance Form

ARAŞTIRMAYA GÖNÜLLÜ KATILIM FORMU

Bu çalışma, Orta Doğu Teknik Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü öğretim üyelerinden Ömer Delialioğlu danışmanlığında Boran Koca tarafından yürütülmektedir. Bu form, sizi araştırma hakkında bilgilendirmek ve gönüllü katılımınızı sağlamak için hazırlanmıştır.

Çalışmanın Amacı Nedir?

Bu araştırma, öğretmenlerin çevrimiçi dayanıklılık düzeylerini ve NIST Siber Güvenlik Çerçevesi bağlamında dijital güvenlik farkındalıklarını değerlendirmeyi amaçlamaktadır. Araştırmadan elde edilen bulgular, eğitim süreçlerinde siber güvenliği artırmaya ve dijital tehditlere karşı daha dayanıklı bir eğitim ortamı oluşturulmasına katkı sağlayacaktır.

Bize Nasıl Yardımcı Olmanızı İsteyeceğiz?

Araştırmaya katılım, çevrimiçi bir anketin doldurulması şeklinde olacaktır. Anket formunun tamamlanması yaklaşık 10-15 dakika sürecek olup, sorular öğretmenlerin dijital güvenlik farkındalıkları ve dayanıklılık stratejileri ile ilgilidir.

Katılımınızla İlgili Bilmeniz Gerekenler:

- Çalışmaya katılmak tamamen gönüllülük esasına dayalıdır. Herhangi bir yaptırım olmaksızın çalışmaya katılmayı reddedebilir veya istediğiniz zaman katılımınızı sonlandırabilirsiniz.
- Araştırma süresince verdiğiniz yanıtlar anonim olarak değerlendirilecek ve yalnızca bu çalışmanın amacı doğrultusunda kullanılacaktır.
- Katılımcılardan toplanan veriler tamamen gizli tutulacak ve üçüncü kişilerle paylaşılmayacaktır. Araştırmanın sonuçları bilimsel ve profesyonel yayınlarda kullanılabilir, ancak hiçbir şekilde katılımcıların kimlik bilgileri açıklanmayacaktır.

Araştırmayla İlgili Daha Fazla Bilgi Almak İsterseniz:

Sorularınız ve yorumlarınız için araştırmacıya şu e-posta adresinden ulaşabilirsiniz:

Onay:

Yukarıdaki bilgileri okudum ve bu çalışmaya tamamen gönüllü olarak katılmayı kabul ediyorum.

Ad Soyad:

Tarih:

İmza:

B. Invitation Form

Duyuru Metni

Sevgili Öğretmenim,

Dijital eğitim araçlarını kullanma ve siber güvenlik konusundaki dijital dayanıklılığınızı değerlendirmek amacıyla hazırlanan bir araştırmaya katkıda bulunmaya davetlisiniz. Bu çalışma, elde edilecek bulgularla eğitim süreçlerinde dijital güvenliği artırmayı ve olası siber tehditlere karşı daha dayanıklı bir ortam oluşturmayı hedeflemektedir.

Formun tamamlanması yaklaşık 10-15 dakika sürecek olup, sorulara verdiğiniz samimi yanıtlar, etkili çözümler üretmemize destek olacaktır. Verileriniz kesinlikle gizli tutulacak, yalnızca bu araştırmanın amacı doğrultusunda kullanılacak ve üçüncü kişilerle paylaşılmayacaktır. Kimlik bilgileriniz toplanmayacak olup, yanıtlarınız tamamen anonim olarak değerlendirilecektir.

Eğitimdeki liderliğiniz ve desteğiniz, öğrencilerimizin ve eğitim sistemimizin dijital güvenliğini güçlendirmede hayati bir rol oynamaktadır. Katılımınız bizim için büyük bir değer taşımaktadır. Şimdiden teşekkür eder, anketimize katılımınızı rica ederiz.

Ankete katılmak için lütfen aşağıdaki bağlantıya tıklayın:

Saygılarımızla,

C. Cyber Resilience Story Form for Teachers (CRSFT) Ethics

Öğretmenler için Siber Dayanıklılık Hikâye Formu

Sevgili öğretmenim

Bu çalışma, dijital eğitim araçlarını kullanma ve siber güvenlik konusundaki dijital dayanıklılığınızı değerlendirmek amacıyla hazırlanmıştır. Bu araştırmadan elde edilecek bulgular, eğitim süreçlerinde dijital güvenliği artırmak ve olası siber tehditlere karşı daha dayanıklı bir ortam oluşturmak amacıyla yapılacak çalışmalara katkı sağlayacaktır. Formun tamamlanması yaklaşık olarak 10-15 dakika sürecektir. Sorulara verdiğiniz gerçek ve samimi yanıtlar, etkili çözümler üretmemize destek olacaktır. Verileriniz gizli tutulacak ve sadece bu çalışmanın amacı doğrultusunda kullanılacaktır. Kimlik bilgileriniz toplanmayacak olup, verdiğiniz yanıtlar tamamen anonim olarak değerlendirilecektir. Veriler, yalnızca bu araştırma kapsamında kullanılacak ve üçüncü kişilerle paylaşılmayacaktır.
Eğitimdeki liderliğiniz, geleceğimizin güvencesidir. Siz değerli öğretmenlerimizin katkıları hem öğrencilerimizin hem de eğitim sistemimizin dijital güvenliğini ve dayanıklılığını güçlendirmede hayati öneme sahiptir. Katılımınız ve desteğiniz için şimdiden teşekkür ederiz.

Branş:	**Eğitimde hangi dijital araçları kullanıyorsunuz?**
Cinsiyet:	**Eğitimde hangi dijital yazılımları kullanıyorsunuz?**
Hangi öğretim seviyesine ders veriyorsunuz:	**Siber Güvenlikle ilgili eğitim ya da ders aldınız mı?**
Eğitim Durumu (Lisans, Y.lisans, Doktora):	**Kurum, içerik, ders saati, memnuniyet durumunuz vb. ile ilgili bilgi verir misiniz?**
Mesleki Deneyim: …. Yıl	
Günlük internet kullanım süreniz: …... Saat	

Yaşanmış Hikayelerden: Peki siz ne yapardınız?

Öğrencileriniz için çok etkili ve eğlenceli materyaller hazırlamışsınız ve onlarla paylaşmak için ders saatini iple çekiyorsunuz. Öğretmenler odasına geçtiniz ve telefonunuzdan okulun internet ağına bağlandınız. Ders saati geldiğinde şahsi bilgisayarınızı alıp sınıfa geçtiniz. Öğrencilerinizle sohbet ederken bir yandan da internete bağlandınız ve diğer hazırlıklarınızı tamamladınız. "Evet çocuklar, bugünkü konumuz için size çok güzel video ve grafikler hazırladım. Önce kısa bir video izleyip konumuza giriş yapalım" dediniz ve video dosyasını açtınız. Ancak ekrana video yerine kıpkırmızı bir ekran geldi. Öğrencileriniz "öğretmenim video açacaktınız, yanlış açtınız" diye sizi uyarmak istediler. Siz de anlam veremediniz, çünkü doğru dosyayı açtığınızdan emindiniz. Bu ekranı kapatıp tekrar video dosyasını açmak istediğinizde yine aynı ekranla karşılaştınız. Öğrencileriniz endişelenmeye başladı, fark ettirmek istemeseniz de sizde endişelendiniz. Çünkü ekrandaki mesajda dosyaların şifresini çözmek için belirli bir miktar fidyenin ödenmesi gerektiği yazıyordu. Dosyalarınıza tekrar baktığınızda her birinin üzerinde bir kilit olduğunuzu fark ettiniz. Öğrencileriniz merakla sormaya başladı: Öğretmenim ne yapacaksınız?

1. **Öğretmen** olarak bilgisayarınızda hangi tür verilerin **en kritik** olduğunu nasıl belirlersiniz?
   a. Bu tehdit **varlıklarınızı** nasıl etkilemiş olabilir?
2. Bu tür bir fidye yazılımı saldırısından **korunmak** için önceden almanız gereken **güvenlik önlemleri** neler olmalıydı?
   a. Önemli dosyalarınızın **yedeklerini** nasıl ve nerede **saklamalısınız**?
3. Bu saldırının belirtilerini daha **erken fark etmek** için hangi tür güvenlik yazılımları veya protokoller kullanılabilir?
   a. İnternete bağlandığınız anda bilgisayarınızda anormal bir durum olup olmadığını nasıl **kontrol** edebilirsiniz?
4. Bu fidye yazılımı saldırısına karşı **ilk yapmanız** gereken şey ne olmalıdır?
   a. Saldırıyı öğrencilere fark ettirmeden yönetmek ve durumu kontrol altına almak için nasıl bir strateji izlersiniz?
5. Saldırıdan sonra dosyalarınızı **geri almanın** mümkün olup olmadığını nasıl belirlersiniz?
   a. Bu olaydan sonra bilgisayarınızı ve verilerinizi nasıl geri yükleyip tekrar güvenli hale getirirsiniz?
6. Eklemek istediğiniz bir şey var mı?

D. Ethics

UYGULAMALI ETİK ARAŞTIRMA MERKEZİ
APPLIED ETHICS RESEARCH CENTER

ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

DUMLUPINAR BULVARI 06800
ÇANKAYA ANKARA/TURKEY
T: +90 312 210 22 91
F: +90 312 210 79 59
ueam@metu.edu.tr
www.ueam.metu.edu.tr

21 OCAK 2025

Konu: Değerlendirme Sonucu

Gönderen: ODTÜ İnsan Araştırmaları Etik Kurulu (İAEK)

İlgi: İnsan Araştırmaları Etik Kurulu Başvurusu

Sayın Ömer DELİALİOĞLU

Danışmanlığını yürüttüğünüz Boran KOCA'nın ***"Sınıf Öğretmenlerinin Siber Dayanıklıklarının Ulusal Standartlar ve Teknoloji Enstitüsü Siber Güvenlik Çercevesi Kapsamında İncelenmesi"*** başlıklı araştırmanız İnsan Araştırmaları Etik Kurulu tarafından uygun görülerek **0017-ODTUİAEK-2025** protokol numarası ile onaylanmıştır

Bilgilerinize saygılarımla sunarım

Prof. Dr. Ş. Halil TURAN
Başkan

Prof.Dr. I. Semih AKÇOMAK
Üye

Doç. Dr. Ali Emre Turgut
Üye

Doç. Dr. Aslı KILIÇ OZHAN
Üye

Doç.Dr. Murat Perit ÇAKIR
Üye

Dr. Öğretim Üyesi Süreyya ÖZCAN KABASAKAL
Üye

Dr. Öğretim Üyesi Müge GÜNDÜZ
Üye

E. Rubrik

Fonksiyon	Soru	Puan	Düzey	Açıklama	Örnek Cevaplar (Öğretmen Cevaplarından ve Literatürden)
Tanımlama	Öğretmen olarak bilgisayarınızda hangi tür verilere en çok önemi verirsiniz? (Örnek: Öğrenci notları, kişisel bilgiler, okulun mali verileri, vb.)	3	Yüksek	En az üç farklı kritik veri türünü (öğrenci kişisel bilgileri, notlar, performans kayıtları, özel eğitim ihtiyaçları, okulun mali verileri, öğrenci/personel fotoğrafları/videoları, rehberlik bilgileri, vb.) açıkça tanımlar.	"Öğrencilerimin kimlik bilgileri, fotoğrafları, notları, devamsızlık bilgileri ve özel eğitim raporları."
		2	Orta	İki farklı kritik veri türünü tanımlar.	"Öğrencilerin kişisel bilgileri ve notları."
		1	Düşük	Yalnızca bir kritik veri türünü tanımlar veya çok genel ifadeler kullanır ("kişisel bilgiler", "özel dosyalar" vb.), somut örnekler vermez.	"Kişisel bilgilerim.", "Özel dosyalarım."
		0	Çok Düşük/Yok	Cevap vermez, konuyla ilgisiz cevap verir veya "Bilmiyorum" der.	"Bilmiyorum", "Fikrim yok", "Önemli bir verim yok."
	Bir fidye yazılımı saldırısı, bilgisayarınızdaki bu kritik verilere ve okulun sistemlerine ne gibi zararlar verebilir? (Örnek: Verilerin şifrelenmesi, çalınması, sistemlerin çökmesi, vb.)	3	Yüksek	Fidye yazılımı saldırısının en az üç farklı olası zararını/etkisini (verilerin şifrelenmesi, çalınması, silinmesi, kimlik hırsızlığı, özel bilgilerin ifşası, okul itibarının zedelenmesi, eğitim süreçlerinin aksaması, mali kayıplar, sistemlerin çökmesi, hesapların ele geçirilmesi vb.) açık ve ayrıntılı bir şekilde tanımlar.	"Öğrenci notları şifrelenebilir, kişisel bilgiler çalınabilir, okulun e-posta sistemi çökertilebilir ve eğitim materyallerine erişim engellenebilir."
		2	Orta	Fidye yazılımı saldırısının iki farklı olası zararını/etkisini tanımlar.	"Verilerim çalınabilir ve bilgisayarım kullanılamaz hale gelebilir."
		1	Düşük	Fidye yazılımı saldırısının yalnızca bir olası zararını/etkisini tanımlar veya tehdidin etkilerini çok genel ifadelerle belirtir, somut örnekler vermez.	"Bilgisayarım bozulabilir.", "Virüs bulaşır."
		0	Çok Düşük/Yok	Cevap vermez, konuyla ilgisiz cevap verir veya "Bilmiyorum" der.	"Bilmiyorum", "Fikrim yok"
Koruma	Bu tür bir fidye yazılımı saldırısından korunmak için bilgisayarınızda ve dijital ortamda ne gibi önlemler alırsınız? (Örnek: Güçlü parola kullanmak, antivirüs yazılımı yüklemek, vb.)	3	Yüksek	Fidye yazılımı saldırılarından korunmak için en az beş farklı önlemi (güçlü ve benzersiz parolalar, iki faktörlü kimlik doğrulama, güvenlik duvarı (firewall), güncel antivirüs yazılımı, düzenli sistem/yazılım güncellemeleri, hassas verilerin şifrelenmesi, düzenli yedekleme (hem yerel hem bulut), bilinmeyen e-postalara/linklere tıklamama, güvenli internet kullanımı, lisanslı yazılım kullanma, siber güvenlik eğitimleri alma, vb.) açıklar.	"Güçlü ve benzersiz parolalar kullanırım, iki faktörlü kimlik doğrulamayı etkinleştiririm, güvenlik duvarımı her zaman açık tutarım, güncel bir antivirüs yazılımı kullanırım, sistemimi ve yazılımlarımı düzenli olarak güncellerim, hassas verilerimi şifrelerim hem bilgisayarıma hem de bulut hesabıma düzenli olarak yedekleme yaparım..."
		2	Orta	Fidye yazılımı saldırılarından korunmak için üç veya dört farklı önlemi belirtir.	"Güçlü parolalar kullanırım, antivirüs programım var ve bilmediğim e-postaları açmam.", "Virüs programı kullanırım, güvenilir sitelere girerim ve dosyalarımı yedeklerim."
		1	Düşük	Fidye yazılımı saldırılarından korunmak için yalnızca bir veya iki önlemden bahseder veya çok genel, yetersiz önlemlerden bahseder.	"Dikkatli olurum.", "Bilinmeyen sitelere girmem.", "Şifre kullanırım."
		0	Çok Düşük/Yok	Cevap vermez, ilgisiz cevap verir veya "Bilmiyorum" der.	"Bilmiyorum", "Fikrim yok"
	Önemli dosyalarınızın yedeklerini nasıl ve nerede saklarsınız? (Örnek: Düzenli aralıklarla harici diske ve bulut hesabına yedekleme, vb.)	3	Yüksek	Yedeklemenin hem nasıl (düzenli aralıklarla, otomatik yedekleme araçları kullanarak, yedekleri test ederek, vb.) hem de nerede (birden fazla güvenli ortamda - hem harici fiziksel depolama biriminde (şifreli) hem de güvenli bulut depolama hizmetinde) yapılması gerektiğini açıklar.	"Önemli dosyalarımı hem harici bir hard diske hem de güvenilir bir bulut depolama hizmetine (örneğin, Google Drive) düzenli aralıklarla (örneğin, haftalık) yedeklerim. Yedekleme işlemini otomatikleştiririm ve yedeklerin çalışıp çalışmadığını düzenli olarak test ederim."
		2	Orta	Yedeklemenin nerede yapılması gerektiği konusunda bazı doğru bilgiler verir (örneğin, harici disk, USB bellek, bulut depolama), ancak nasıl yapılması gerektiği (düzenli, otomatik, güvenli, vb.) konusunda yetersiz bilgi verir.	"Dosyalarımı harici bir diske yedeklerim.", "Bilgisayarımda ve USB bellekte yedeklerim var."
		1	Düşük	Yedekleme yapılması gerektiğinden genel olarak bahseder, ancak nasıl ve nerede yapılması gerektiği konusunda çok az bilgi verir veya yanlış bilgi verir (örneğin, sadece bilgisayarın içinde yedeklemek).	"Bilgisayarımda yedeklerim.", "Başka bir dosyaya kaydederim."
		0	Çok Düşük/Yok	Cevap vermez, ilgisiz cevap verir, "Bilmiyorum" der veya yedekleme yapmadığını belirtir.	"Bilmiyorum", "Fikrim yok", "Yedekleme yapmam"

Table Continued

Algılama	Bilgisayarınızda bir fidye yazılımı saldırısının erken belirtileri olabilecek ne tür durumlarla karşılaşabilirsiniz? (Örnek: Bilgisayarın yavaşlaması, bilinmeyen dosyalar, vb.)	3	Yüksek	Fidye yazılımı saldırısının en az üç farklı erken belirtisini (anormal yavaşlama, tanınmayan programlar/dosyalar, dosyaların açılamaması veya uzantılarının değişmesi, şifreleme uyarıları, anormal ağ trafiği, beklenmeyen pop-up'lar, antivirüs uyarıları, sistem ayarlarının izinsiz değişmesi, vb.) doğru ve birbirinden ayırt edilebilir şekilde tanımlar.	"Bilgisayarım her zamankinden çok daha yavaş çalışmaya başlarsa, açamadığım veya uzantısı .xyz gibi bilmediğim bir uzantıya dönüşmüş dosyalar görürsem, bilmediğim programlar veya pencereler açılırsa ve antivirüs programım sürekli uyarı verirse şüphelenirim."
		2	Orta	Fidye yazılımı saldırısının iki farklı erken belirtisini tanımlar.	"Bilgisayarım yavaşlarsa ve antivirüs programım uyarı verirse şüphelenirim.", "Bilgisayarımda bilinmeyen dosyalar görürsem ve dosyalarım açılmazsa anlarım."
		1	Düşük	Fidye yazılımı saldırısının yalnızca bir erken belirtisini tanımlar veya çok genel, yanlış veya yetersiz belirtilerden bahseder.	"Virüs çıkarsa anlarım.", "Bilgisayarım bozulursa anlarım.", "Kısıtlama olursa anlarım."
		0	Çok Düşük/Yok	Cevap vermez, ilgisiz cevap verir, "Bilmiyorum" der veya herhangi bir göstergeye dikkat etmediğini belirtir.	"Bilmiyorum", "Fikrim yok"
	İnternete bağlandığınız anda, bilgisayarınızda şüpheli bir e-posta, tanımadığınız bir programın çalışması veya dosyalarınızın açılmaması gibi anormal bir durum fark ederseniz hemen ne yaparsınız?	3	Yüksek	Anormal durumu fark ettikten sonra hemen yapılması gereken en az üç doğru eylemi (internet bağlantısını kesmek, bilgisayarı kapatmak/uyku moduna almak, yetkililere/BT ekibine/okul yönetimine haber vermek, antivirüs taraması yapmak/güncellemek, şüpheli işlemleri durdurmak, yedekleri kontrol etmek, vb.) öncelik sırasını gözeterek ve mantıklı bir şekilde açıklar.	"Hemen internet bağlantımı keserim (kablosuz ağı kapatır veya ethernet kablosunu çekerim), bilgisayarı güvenli modda yeniden başlatırım ve okulun bilişim teknolojileri (BT) ekibine hemen haber veririm. Durumu ayrıntılı olarak anlatır, onların yönlendirmelerine göre hareket ederim."
		2	Orta	Anormal durumu fark ettikten sonra yapılması gereken iki doğru eylemi belirtir.	"Bilgisayarımı kapatırım ve virüs taraması yaparım.", "BT ekibine haber veririm ve bilgisayarı yeniden başlatırım."
		1	Düşük	Anormal durumu fark ettikten sonra yapılması gereken yalnızca bir doğru eylemi belirtir veya çok genel, yetersiz veya yanlış eylemlerden bahseder.	"Tekrar açarım.", "Ekranda bir değişiklik olursa farkederim.", "Virüs programına bakarım."
		0	Çok Düşük/Yok	Cevap vermez, ilgisiz cevap verir, "Bilmiyorum" der veya herhangi bir eylemde bulunmayacağını belirtir.	"Bilmiyorum", "Fikrim yok", "Bir şey yapmam"

Yanıt Verme	Bir fidye yazılımı saldırısına maruz kaldığınızı fark ettiğiniz anda ilk yapmanız gereken şey nedir? (Örnek: İnternet bağlantısını kesmek, vb.)	3	Yüksek	Fidye yazılımı saldırısı karşısında derhal yapılması gereken en kritik ve doğru eylemleri (ağ bağlantısını/interneti kesmek ve/veya bilgisayarı kapatmak/uyku moduna almak ve yetkililere/BT ekibine/okul yönetimine haber vermek) öncelik sırasına göre ve mantıklı bir şekilde belirtir.	"Hemen bilgisayarımın internet bağlantısını keserim (kablosuz ağı kapatır veya ethernet kablosunu çekerim). Bilgisayarı kapatır ve okulun BT ekibine/müdüre haber veririm."
		2	Orta	Yapılması gereken iki doğru eylemi (örneğin, interneti kapatmak, bilgisayarı kapatmak, yetkililere haber vermek) belirtir.	"Bilgisayarı kapatırım ve BT uzmanına haber veririm.", "Yetkililere haber veririm."
		1	Düşük	Yalnızca bir doğru eylem belirtir veya çok genel, yetersiz, yanlış veya zararlı olabilecek eylemlerden (örneğin, "virüs taraması yapmak", "format atmak", "dosyaları açmaya çalışmak", "şikayet etmek") bahseder.	"Virüs taraması yaparım.", "Çıkabiliyorsam siteden çıkarım."
		0	Çok Düşük/Yok	Cevap vermez, ilgisiz cevap verir, "Bilmiyorum" der veya hiçbir şey yapmayacağını belirtir.	"Bilmiyorum", "Fikrim yok", "Bir şey yapmam"
	Okulunuzda bir fidye yazılımı saldırısı yaşanırken, öğrencilerin bu durumdan en az şekilde etkilenmesini ve derslerin devam etmesini sağlamak için neler yaparsınız?	3	Yüksek	Öğrencilerin paniklemesini önlemek, güvenlerini sağlamak, mahremiyetlerini korumak ve eğitim sürecinin devamlılığını sağlamak için en az üç farklı ve uygun eylemi (sakin kalmak, durumu öğrencilere yaşlarına uygun bir dille açıklamak (veya açıklamamak), alternatif bir etkinlik/materyal/yöntem bulmak, yetkililere (BT ekibi, okul yönetimi) haber vermek, teknik işlemleri (bağlantıyı kesmek, vb.) hızlı ve gizlice yapmak) mantıklı bir sırayla açıklar.	"Sakin kalırım ve öğrencilere teknik bir sorun olduğunu, ancak dersimize devam edeceğimizi söylerim. İnternet bağlantısı gerektirmeyen bir etkinlik bulurum (örneğin, kitaptan okuma, yazma çalışması, grup çalışması). Bu arada, okulun BT ekibine haber verir ve onların yönlendirmelerine göre hareket ederim."
		2	Orta	Öğrencilerin paniklemesini önlemek ve eğitim sürecini devam ettirmek için iki doğru eylemi belirtir.	"Hemen bilgisayarı kapatır, bilişim uzmanına durumu bildiririm.", "İnternet ile ilgili bir sorun yaşandığını söyler, ders işleyişini başka bir yöntemle sürdürürüm."
		1	Düşük	Öğrencilerin paniklemesini önlemek ve eğitim sürecini devam ettirmek için yalnızca bir doğru eylem belirtir veya çok genel, yetersiz, yanlış veya zararlı olabilecek eylemlerden bahseder.	"Öğrencilere anlatırım doğrusu neyse onu", "Sorun yok derim"
		0	Çok Düşük/Yok	Cevap vermez, ilgisiz cevap verir, "Bilmiyorum" der veya hiçbir şey yapmayacağını belirtir.	"Bilmiyorum", "Fikrim yok", "Neden fark ettirmemeye çalışmalıyım?"

Table Continued

Kurtarma	Bir fidye yazılımı saldırısından sonra, şifrelenmiş dosyalarınızı geri almanın mümkün olup olmadığını nasıl değerlendirirsiniz?	3	Yüksek	Dosyaları geri almanın mümkün olup olmadığını değerlendirmek için en az üç farklı ve doğru yöntemi (dosyaların gerçekten şifrelenip şifrelenmediğini ve hangi tür şifreleme kullanıldığını kontrol etmek, yedeklerin (varsa) güncel, sağlam ve erişilebilir olup olmadığını kontrol etmek, profesyonel veri kurtarma hizmetlerini/yazılımlarını araştırmak, yetkililere (BT ekibi, okul yönetimi, siber güvenlik uzmanları) danışmak) mantıklı bir sırayla ve ayrıntılı olarak açıklar.	"Öncelikle dosyaların gerçekten şifrelenip şifrelenmediğini ve hangi tür şifreleme kullanıldığını kontrol ederim. Daha sonra, en son yedeğimin ne zaman alındığını, nerede saklandığını ve sağlam olup olmadığını kontrol ederim. Eğer yedeklerim varsa, dosyaları yedekten geri yüklemeyi denerim..."
		2	Orta	Dosyaları geri almanın mümkün olup olmadığını değerlendirmek için iki doğru yöntemi belirtir.	"Dosyaların şifrelenip şifrelenmediğine bakarım ve yedeklerimi kontrol ederim.", "Virüs taraması yapar ve bazı uygulamaları denerim."
		1	Düşük	Dosyaları geri almanın mümkün olup olmadığını değerlendirmek için yalnızca bir doğru yöntem belirtir veya çok genel, yetersiz, yanlış veya zararlı olabilecek yöntemlerden bahseder.	"Tekrar açmayı denerim.", "Format atarım."
		0	Çok Düşük/Yok	Cevap vermez, ilgisiz cevap verir, "Bilmiyorum" der, hiçbir şey yapmayacağını belirtir veya dosyaların kesinlikle geri alınamayacağını düşünür.	"Bilmiyorum", "Fikrim yok", "Geri almam"
	Fidye yazılımı saldırısından sonra, hem bilgisayarınızı hem de verilerinizi (mümkünse) en güvenli şekilde nasıl kurtarırsınız? (Örnek: Yedeklerden geri yükleme, sistemi yeniden kurma, vb.)	3	Yüksek	Veri ve sistemi kurtarmak için en az üç farklı ve doğru yöntemi (varsa güncel ve güvenli yedeklerden geri yüklemek, sistemi güvenli modda başlatmak, güncel bir antivirüs yazılımı ile tam sistem taraması yapmak, gerekirse profesyonel yardım almak, gerekirse sistemi temiz bir şekilde yeniden kurmak (formatlamak), güvenlik açıklarını kapatmak için sistem ve yazılımları güncellemek, güçlü parolalar kullanmak, vb.) mantıklı bir sırayla ve ayrıntılı olarak açıklar.	"*Öncelikle bilgisayarımı güvenli modda başlatır ve güncel bir antivirüs yazılımı ile tam sistem taraması yaparım. Eğer virüs temizlenemezse veya sistem hala düzgün çalışmıyorsa, en son yedeğimden verilerimi geri yüklerim. Eğer yedeğim yoksa, profesyonel bir veri kurtarma hizmetinden yardım alırım. Son çare olarak, bilgisayarıma temiz bir kurulum (format) yapar ve işletim sistemini ve tüm yazılımları yeniden yüklerim..."
		2	Orta	Veri ve sistemi kurtarmak için iki doğru yöntemi belirtir.	"Yedeklerimden verilerimi geri yüklerim ve virüs taraması yaparım.", "Format atarım ve sistemi yeniden kurarım."
		1	Düşük	Veri ve sistemi kurtarmak için yalnızca bir doğru yöntem belirtir veya çok genel, yetersiz, yanlış veya zararlı olabilecek yöntemlerden bahseder.	"Bilgisayarcıya götürürüm.", "Yeniden başlatırım."
		0	Çok Düşük/Yok	Cevap vermez, ilgisiz cevap verir, "Bilmiyorum" der veya hiçbir şey yapmayacağını belirtir.	"Bilmiyorum", "Fikrim yok", "Bir şey yapmam"