International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

INTERNATIONAL JOURNAL OF MODERN EDUCATION (IJMOE)
www.ijmoe.com

GLOBAL ACADEMIC EXCELLENCE

STRENGTHENING EDUCATIONAL SYSTEMS THROUGH DATA INTEGRITY: INSIGHTS FROM THE MINISTRY OF EDUCATION MALAYSIA'S DATA CENTER

Azlin Ramli[1*], Mohamad Yusof Darus[2], Othman Talib[3], Azliza Yacob[4]

[1] College of Computing, Informatics and Mathematics, Universiti Teknologi MARA (UiTM), 40450 Shah Alam, Selangor Darul Ehsan, Malaysia
Email: 2023939969@student.uitm.edu.my
[2] College of Computing, Informatics and Mathematics, Universiti Teknologi MARA (UiTM), 40450 Shah Alam, Selangor Darul Ehsan, Malaysia
Email: yusof_darus@uitm.edu.my
[3] Faculty of Social Science and Liberal Arts, UCSI University, Taman Connaught, 56000 Kuala Lumpur, Malaysia
Email: othmantalib@UCSIuniversity.edu.my
[4] Faculty of Computer, Media & Tech. Management, University College TATI (UC TATI), Kampus TATIUC, Teluk Kalong, 24000 Terengganu, Malaysia
Email: azliza@uctati.edu.my
[*] Corresponding Author

Article Info:

Article history:
Received date: 30.06.2024
Revised date: 17.07.2022
Accepted date: 28.08.2024
Published date: 30.09.2024

To cite this document:

Ramli, A., Darus, M. Y., Talib, O., & Yacob, A. (2024). Strengthening Educational Systems Through Data Integrity: Insights From The Ministry Of Education Malaysia's Data Center. *International Journal of Modern Education, 6* (22), 482-501.

DOI: 10.35631/IJMOE.622033

Abstract:

It examines the factors that affect data integrity in the Data Center of the Ministry of Education Malaysia (KPM) and analyzes the effectiveness of existing security measures. By ensuring data integrity, educational systems can be strengthened, leading to more reliable and effective decision-making processes. This, in turn, supports the overall goal of enhancing educational outcomes. This study uses a qualitative research approach by interviewing five civil servants related to the management of government data centers. The findings of the study show that there are several weaknesses in the management of cyber security in data centers, including lack of training and security awareness, insufficient monitoring and periodic audits, as well as lack of support and commitment from superiors. In addition, this study also found that the existing cyber security policy is not strict and clear enough, and investment in security technology is still low. Based on these findings, the ENSTEK Data Center Data Security and Integrity model has been developed to overcome these weaknesses. This model contains the components of security training and awareness, regular monitoring and audits, investment in security technology, strict and clear cyber security policies, and support and commitment from the top. This model is expected to improve the security and integrity of data in government data centers as well as provide important guidance for further research in the field of cyber security.

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

Keywords:

Cybersecurity, Cyber Security Policy, Data Center, Data Integrity, Malaysian Ministry of Education, Security Management

Introduction

In this highly sophisticated digital era, cyber security is a very critical aspect for any organization, including the Malaysian Ministry of Education (KPM). KPM's ENSTEK Data Center is an important data storage and management center to ensure the continuity of education operations throughout the country. However, these data centers are facing a major challenge due to the absence of a comprehensive ICT security framework.

In the rapidly developing digital era, ICT security has become an important element in ensuring data integrity, especially in the public sector. The Malaysian Ministry of Education's (KPM) Data Center plays a critical role in the management and protection of sensitive data. However, there are various challenges faced, such as a lack of expertise among civil servants and a low level of information security awareness (ISA)(Bolger et al., 2023). This can lead to weaknesses in compliance with established security protocols, thereby increasing the risk to data integrity. Therefore, this study aims to explore the factors that contribute to ICT security issues at the KPM Data Center and suggest measures to strengthen security compliance and improve data integrity.

The absence of a comprehensive ICT security framework at the KPM ENSTEK Data Center causes efforts to protect data and ICT systems to be disorganized and less effective. This leads to weak cyber security management and an inability to deal with increasingly sophisticated cyber threats. Without clear and comprehensive guidance, staff may take different approaches to safety, resulting in confusion and inconsistencies in safety practices. Safety standards and procedures that are not clearly defined also cause the level of standardization of safety measures to be too low. Efforts to protect data become ineffective without a comprehensive security framework, which ultimately increases variability in security approaches(Dioubate et al., 2023).

Based on the problems identified, this study has two specific objectives: to identify factors that contribute to weaknesses in cyber security management at the ENSTEK Data Center of the Ministry of Education Malaysia and to analyze the level of effectiveness of existing security measures in protecting data and ICT systems at the ENSTEK Data Center of the Malaysian Ministry of Education.

Cybersecurity is essential in ensuring data integrity, availability, and confidentiality in any organization (Admass et al., 2024; Kitsios et al., 2022) These threats include hacker attacks, malware, and DDoS (Distributed Denial of Service) attacks that can disrupt the operation of ICT systems and affect important data (Shammugam et al., 2021).

KPM's ENSTEK Data Center is not exempt from facing these threats. However, without a comprehensive ICT security framework, measures to address these threats become disorganized. According to various studies, the lack of a clear framework causes staff not to have the right guidance to implement effective security measures. This leads to inconsistencies

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

in implementing security measures that can open space for cyberattacks (Mtukushe et al., 2023).

This study is important because it aims to fill the gap in understanding the factors contributing to cyber security vulnerabilities at the KPM ENSTEK Data Center. By identifying these factors, we can build a more effective and organized ICT security framework. Additionally, this study will analyze the effectiveness of existing security measures, which can aid in their improvement. Ensuring the protection of data and ICT systems from increasingly sophisticated cyber threats is crucial.

To produce statistical tables for ICT security problems in the Malaysian Ministry of Education's Data Center, it requires empirical data collected through questionnaires, interviews, or related secondary sources. Here is a hypothetical example of a statistical table that might help outline the main issues, based on the factors identified in the ICT security study.

Table 1. ICT Security problems in the Malaysian Ministry of Education's Data Center

Problem Factors	Number of Respondents (%)	Level of Consciousness	Importance
Lack of Technology Expertise	65	Low	High
Information Security Awareness (ISA)	50	Medium	High
Security Protocol Non-compliance	45	Low	Medium
Lack of Support Infrastructure	40	High	High
Cyber Attacks (Phishing, Malware)	35	Low	High

This study will use a qualitative approach by conducting in-depth interviews and document analysis to identify factors that contribute to weaknesses in cyber security management. We will conduct interviews with ICT security management staff at KPM's ENSTEK Data Center. We will analyze the obtained data to identify the main themes related to cyber security vulnerabilities. Furthermore, this study will scrutinize the implemented security measures (Tzavara & Vassiliadis, 2024).

Through this study, we hope to identify the main factors contributing to cyber security management weaknesses at KPM's ENSTEK Data Center. We also expect this study to provide a clearer picture of the effectiveness of existing security measures. MOE's ENSTEK Data Center and other data centers in the Malaysian public sector can utilize the study's results to construct a more comprehensive and effective ICT security framework.

Cybersecurity is a critical aspect of data management and ICT systems, especially in educational institutions such as KPM. To ensure the security of data and ICT systems, we must address the major challenge of the absence of a comprehensive ICT security framework (Rao et al., 2023). Ensuring data integrity is crucial for the effective functioning of educational systems, as it supports reliable decision-making and enhances educational outcomes. By addressing these challenges, the Ministry of Education Malaysia can significantly strengthen

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

its educational infrastructure. This study also aims to identify factors that contribute to weaknesses in cybersecurity management.

Literature Review

The following is an example of a table summarizing the findings of previous studies on ICT security and data integrity in data centers, particularly in the context of Malaysia's public sector:

Table 2. Summarizing The Previous Study

Author/Year	Study Topic	Key Findings	Proposal
(Nor Kamaliah Mohammad et al., 2014)	Data Security in Malaysian Government Data Centers	Lack of information security awareness (ISA) among government employees causes data risks.	Increased security training and development of cyber awareness among civil servants.
(Maniam & Singh, 2020)	ICT Security Framework for the Education Sector	Existing ICT security systems are not comprehensive to deal with the latest cyber threats.	Integrating a risk-based data security framework in data center management in the education sector.
(Lee & Ariffin, 2021)	Awareness of ICT Security Policy in Malaysian Government Agencies	Awareness of ICT security policy is still at a moderate level, causing non-compliance with existing protocols.	Stricter enforcement and improvement of information security policies for government agencies.
(Lee et al., 2021)	Cyber Security in the Malaysian Public Sector	Phishing and malware are the main threats that often occur in public sector data centers.	Use of more sophisticated cyber threat detection and prevention tools in public sector data centers.

Based on the title of the article, problem statement, and specific objectives of the study, the following are the things that need to be discussed in the Literature Review section.

Cyber Security and Data Integrity in Government Data Centers

This section explores into the critical relationship between cyber security and data integrity within government data centers.

a) Examining the existing literature on the cyber security risks that government data centers encounter.
b) Discuss the importance of data integrity in the context of government data centers and the impact of weaknesses in cyber security management on data integrity.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

ICT Security Framework

This section explores various ICT security frameworks and their effectiveness in safeguarding data and ICT systems.

a) Examine the different ICT security frameworks that other organizations have created and implemented.
b) Assess the effectiveness of the framework in protecting data and ICT systems from cyber threats.
c) This article discusses the important elements of a comprehensive ICT security framework.

Factors Contributing to Cyber Security Weaknesses

This section examines the multifaceted factors that contribute to cyber security weaknesses in data centers.

a) This study examines the factors that contribute to weaknesses in cyber security management, including human, technology, and process factors.
b) The article discusses previous studies that have identified these weaknesses and the steps taken to overcome them.

An Evaluation of the Efficiency of Current Security Measures

This section provides an analysis of the current security measures in place and their effectiveness in protecting data centers.

a) Examine the research on the efficacy of the security measures used in government data centers.
b) Assess the extent to which these measures can protect data and ICT systems from cyber threats.
c) Discuss case studies or specific examples where security measures have succeeded or failed.

Comprehensive Review of Cyber Attacks and Security Challenges

This section offers a comprehensive review of the types of cyber-attacks and security challenges faced by data centers.

a) This study examines common types of cyberattacks and security challenges faced by data centers.
b) This article discusses the latest trends in cyber threats and the strategies used to counter them.

Recent Studies in Data and Device Security

This section reviews the latest research on data and device security, focusing on emerging technologies and trends**.**

a) Review the most recent research on data and device security, including IoT research and new cyber security technologies.

The Importance of System Security Management and Cyber Risk Assessment

This section highlights the importance of system security management and cyber risk assessment in maintaining data integrity.

a) Discuss the importance of system security management and risk assessment in ensuring data security and integrity.
b) This study delves into the methodology of cyber risk assessment and explores its application within the framework of government data centers.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

This literature review aims to examine and evaluate various aspects related to cyber security and data integrity in government data centers. To understand these issues, it is important to review previous literature that has examined cyber security, ICT security frameworks, and factors that contribute to cyber security vulnerabilities. Ensuring data integrity is crucial for the effective functioning of educational systems, as it supports reliable decision-making and enhances educational outcomes. By addressing these challenges, the Ministry of Education Malaysia can significantly strengthen its educational infrastructure.

This study begins with an introduction to the literature on cyber security and data integrity. Cybersecurity is an area that is receiving more attention in this digital age due to the increase in cyberattacks that can affect data integrity, availability, and confidentiality. Previous studies have shown that government data centers are often the target of cyber-attacks because they store critical and sensitive data(Hamdah et al., 2024). Therefore, a deep understanding of cyber security threats and measures to deal with them is essential to ensure data security in government data centers (Anthony Anyanwu et al., 2024)

The main themes in this literature review include cyber security threats, ICT security frameworks, and factors that contribute to weaknesses in cyber security management. Cyber security threats include various types of attacks such as malware, DDoS attacks, and hacking. Previous studies also emphasize the importance of a comprehensive ICT security framework to protect data and ICT systems from these threats. An effective ICT security framework needs to include elements such as security policies, access control, risk management, and cyber security training for staff.

We need to fill several research gaps to enhance our understanding of cybersecurity in government data centers. Among them is the lack of in-depth research on the specific factors that contribute to weaknesses in cyber security management in government data centers. Furthermore, studies on the effectiveness of implemented security measures and their potential for improvement are scarce. This study aims to fill these gaps by identifying factors that contribute to cybersecurity vulnerabilities and analyzing the effectiveness of existing security measures (Xue et al., 2023).

The formation of a conceptual framework is important to structure this study. The proposed conceptual framework includes three main components: cyber security threats, security vulnerability factors, and security measures. Cybersecurity threats include various types of attacks that can affect the integrity of data (Hazmi et al., 2023). Security weakness factors include a lack of training, access control weaknesses, and non-compliance with security policies. Actions such as strengthening security policies, increasing cyber security training, and implementing more sophisticated security technology are examples of security measures that can protect data and ICT systems (Bolek et al., 2023; Rani et al., 2025).

The main findings in this study show that the lack of a comprehensive ICT security framework is a major factor contributing to weaknesses in cyber security management in government data centers. The study also revealed that despite implementing security measures, there is still room for improvement in their effectiveness. There is controversy over the effectiveness of some security measures, such as the use of antivirus software and firewalls, which may not be sufficient to protect against increasingly sophisticated cyber threats (Dirin, 2023).

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

In conclusion, this literature review emphasizes the importance of a deep understanding of cyber security threats and the factors that contribute to weaknesses in cyber security management in government data center (Cremer et al., 2022). This study also reveals the need to address research gaps to enhance the efficacy of current security measures. It is important to establish a comprehensive conceptual framework to structure this study and ensure that all aspects related to cyber security and data integrity are considered. By enhancing data integrity, educational institutions can ensure more reliable and effective decision-making processes. This, in turn, supports the overall goal of improving academic outcomes and strengthening educational systems. We hope that a deeper understanding of these issues will lead to the implementation of more effective measures to safeguard data and ICT systems in government data centers.

Significance and Contribution

Contribution to the Government

This study can assist the government in identifying and understanding the factors that contribute to the weaknesses in cyber security management at the Malaysian Ministry of Education's ENSTEK Data Center. The government can increase its ability to protect data and ICT systems from increasingly sophisticated cyber threats by using the findings of this study to formulate a more comprehensive and effective cyber security policy. By implementing a stronger security framework, the government can safeguard the integrity, availability, and confidentiality of its data, thereby fostering public trust in its administrative system. By securing educational data, the government can enhance the quality and reliability of educational services, ultimately benefiting students and educators.

Contribution to the Community

This study will benefit the community, particularly those in the education sector, by providing clear guidance on necessary cyber security measures. Better awareness and understanding of cyber security can reduce the risk of cyber threats in educational institutions. Additionally, communities can learn about the importance of keeping personal and institutional data secure, which in turn can improve cyber security at the individual and organizational levels. Enhanced cyber security in educational institutions ensures a safer learning environment, protecting students' and educators' sensitive information.

Contribution to Industry

The study's findings will also benefit the technology and cyber security industries will also benefit from the results of this study. Companies in this industry can use the study's findings to enhance and expand their cybersecurity products and services. By knowing the weaknesses that exist in the management of cyber security in government data centers, these companies can offer more appropriate and effective solutions. This not only improves cyber security in Malaysia, but it also provides the cyber security industry with more business opportunities. Developing robust cyber security solutions for educational data centers can lead to innovations that enhance the overall educational infrastructure.

Contribution to Knowledge

This article contributes new knowledge about cyber security management in government data centers. This study provides a clear picture of the factors that contribute to cyber security weaknesses, as well as the effectiveness of the measures taken. Other researchers interested in

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033
studying cyber security in different contexts can use this finding as a reference. Furthermore, this study serves as a foundation for future research that can aid in the development of a more comprehensive and effective cybersecurity framework. The insights gained from this study can inform educational policies and practices, leading to more secure and efficient management of educational data.

Methodology

This study uses qualitative research methods and has interviewed five participants. This article employs the 'Basic Qualitative Inquiry' research design.

Research Design

We chose the 'Basic Qualitative Inquiry' research design because it effectively addresses the research questions concerning the experiences and perspectives of the participants.

This design allows for an in-depth exploration of the factors that contribute to cybersecurity vulnerabilities and the effectiveness of existing security measures, as well as allows for an in-depth exploration of the factors contributing to cyber security weaknesses in the Ministry of Education Malaysia's Data Center, capturing nuanced perspectives and experiences. It is also in line with the objective of the study to identify and analyze relevant factors(Lim, 2024).

Data Collection

The data collection methods used in this study include in-depth interviews and observations. We prepared a set of interview questions as the main instrument to obtain detailed information from the participants. These interviews contributed to understanding the participants' experiences and views on cyber security in the data center. We use observation to gain a comprehensive understanding of workplace safety practices. This method was chosen in accordance with the study's goal of obtaining deep and rich data on the topic under study.

Sampling

The sampling strategy employed is purposive sampling, specifically targeting civil servants involved in managing government data centers. We chose this technique to select participants with relevant knowledge and experience in the research topic. We selected a sample size of five participants, which we considered sufficient to gather in-depth data for a qualitative study. (Daher, 2023).

Data Analysis

Coding and thematic analysis are the two data analysis techniques used. Analysis was conducted using Atlas.ti software. The coding process involves categorizing the data into relevant themes, whereas thematic analysis helps identify the main patterns and themes in the collected data. This method is suitable for this study because it allows for in-depth exploration of qualitative data and helps to understand complex issues.

Ethical Considerations

We have taken ethical considerations such as obtaining written consent from all participants, maintaining the confidentiality of participant information, and ensuring the use of all collected data solely for research purposes. We also obtained ethical approval from the institutional research ethics committee.

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

Data Validity and Reliability

We have used measures like data triangulation, member checking, and audit trail to ensure the validity and reliability of the data. Triangulation involves using multiple data sources to confirm findings, while member checking allows participants to verify the accuracy of the data collected. Therefore, by employing triangulation, the study enhances the credibility and depth of the findings, providing a more comprehensive understanding of the research topic. The audit trail ensures that all steps in the research process are carefully documented(Indriyanto, 2023).

The objectives and research questions form the basis of this study's methodology overall. The use of qualitative methods allows for an in-depth exploration of the factors that contribute to cyber security vulnerabilities and the effectiveness of security measures. The research design, data collection methods, sampling strategy, data analysis techniques, and ethical considerations all contribute to the effectiveness of this study in achieving its objectives. Figure 1 will elucidate this method.

.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

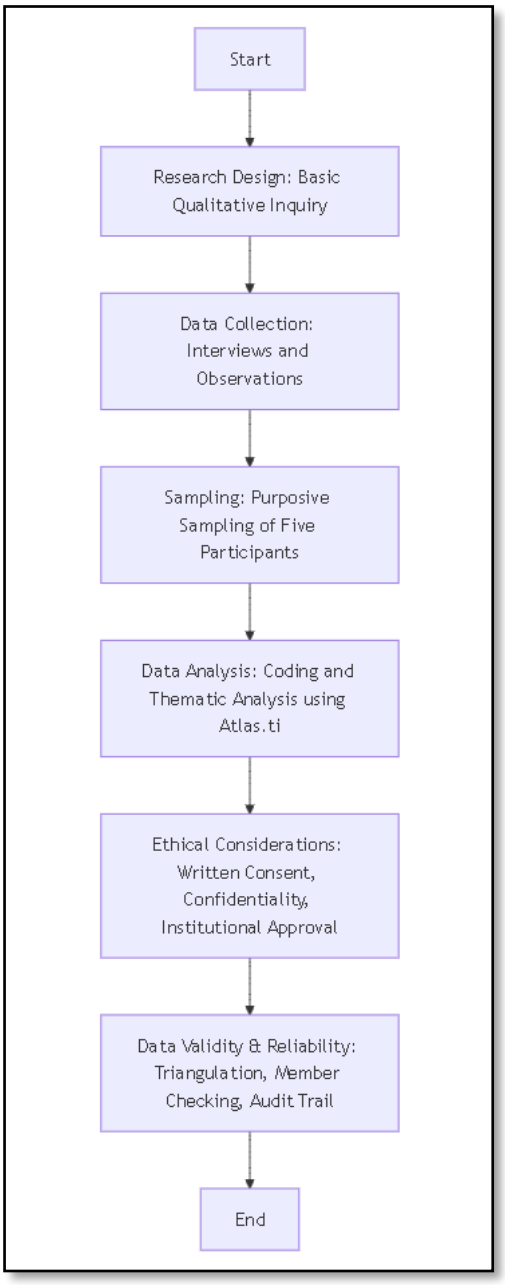

Figure 1. Flow Chart For Methodology

The challenge of data management, especially in the context of data centers and large organizations, involves several critical aspects that need attention.

Maintaining continuous availability of data is one of the major challenges. Data centers should work 24/7 with high uptime to ensure no service interruptions. However, factors such as technical maintenance, system failure, or cyber-attacks can cause downtime that has a major impact on an organization's daily operations.

Cybersecurity threats related to data security, such as hacker attacks, malware, and phishing, are on the rise. Managing data security involves protection against intrusion, data loss, and

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

compliance with privacy laws and regulations. The lack of expertise and security awareness among staff also increases the risk.

Big Data Management focuses on expanding data, where complexity poses challenges in data storage, access, and analysis. Diverse data formats and sources require more advanced technological capabilities to process data quickly and accurately.

To ensure effective and efficient data management, these challenges necessitate strategic planning, technology investment, and enhanced staff skills. We adapted the questionnaire for this study to fit its purpose and the study's context. We have adapted and modified questionnaire instruments from other studies to make them relevant to both the respondents and this study.

Findings

This study conducted interviews with five civil servants who are involved in government data center operations. Several main themes emerged from the conducted interviews, reflecting the participants' views and experiences on cyber security at the ENSTEK Data Center of the Ministry of Education Malaysia. The following are the main themes that have been identified:

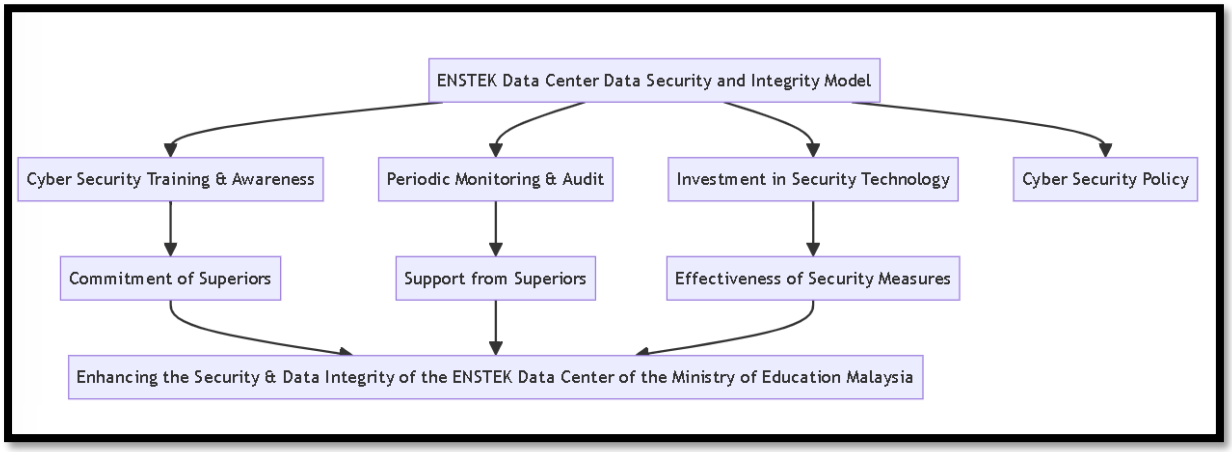

Figure 2: ENSTEK Cyber Security Effectiveness Model

Weaknesses in Cyber Security

Based on the interviews, there are several major weaknesses in cyber security management at the ENSTEK Data Center. Participants underscored the absence of cyber security training for staff. This deficiency causes staff to be less prepared to face increasingly sophisticated cyber threats. Furthermore, irresponsible parties fail to detect system vulnerabilities through periodic monitoring and audits (Anthony Anyanwu et al., 2024). The flowchart clearly indicates that without adequate cyber security training and awareness, staff at ENSTEK Data Center may not fully understand or engage with other critical aspects of the model, such as policy adherence or technology investments.

Challenges in Addressing Cyber Threats

Participants also shared the main challenges faced in maintaining cyber security. One of the most significant challenges is the lack of budget to invest in more sophisticated security technology. Participants also stated that there was difficulty in getting support from superiors in implementing the necessary security measures. In addition, increasingly sophisticated

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033
cyberattacks make efforts to maintain cyber security more challenging(Nadeem et al., 2023). Participants feel that they are often unable to keep up with the latest security technology developments. The model's interconnected nature emphasizes how budget constraints for investment in security technology can have a chain of subsequent effects on other areas such as periodic monitoring and auditing or policy development.

Effectiveness of Existing Security Measures

Regarding the effectiveness of existing security measures, participants' views were mixed. Some participants feel that the measures taken are quite effective, but there is still a lot of room for improvement. Some believe that these measures' efficacy depends on the situation and that much work remains. Participants suggested updating security technology and increasing staff training to improve security measures (Sharma et al., 2023). The central placement of 'Effectiveness of Security Measures' within the flowchart underscores its dependence on both superior support and investment in technology, aligning with participants' views on conditional effectiveness.

Recommendations to Improve Cybersecurity

Participants have given several suggestions to improve cyber security at the ENSTEK Data Center. Among the main recommendations is to increase cyber security training for staff. Participants felt that with better training, staff would be better prepared to face cyber threats. Participants also recommended increasing investments in advanced security technology. Participants also emphasized the importance of periodic audits and monitoring as a crucial step towards ensuring more effective cyber security. This visual representation highlights participants' recommendations by showing that improvements in training, investments, and audits are foundational elements that support an effective cybersecurity policy.

Lack of Cyber Security Awareness

Another important theme identified is the lack of cyber security awareness among staff. Participants felt that awareness of the importance of cyber security is still low, and this makes it difficult to implement effective security measures. They recommended conducting cyber security awareness campaigns more frequently to enhance staff knowledge and comprehension of cyber threats and protective measures for data and ICT systems.

The diagram emphasizes 'Cyber Security Training & Awareness' as a starting point for enhancing data integrity at ENSTEK Data Center, reinforcing participants' concerns about current levels of awareness among staff.

The Importance Of Cyber Security Policy

Participants also emphasized the importance of having a strict and clear cyber security policy. All staff must adhere to this policy to ensure effective cyber security. Participants recommended regularly renewing and updating the cyber security policy to keep it up-to-date with the latest cyber threats. Participants suggest placing the 'Cyber Security Policy' at one end of the model's spectrum to highlight its role as a goalpost for all other measures, thereby stressing its importance.

The Importance Of Receiving Support From Superiors

Support from the top is critical in ensuring the effectiveness of cyber security measures. Participants felt that without this support, efforts to implement security measures would face

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

many obstacles. They suggested that the superiors be more proactive in supporting cyber security efforts and provide a sufficient budget to implement the necessary measures.

The study's overall findings indicate several weaknesses in the cyber security management at the ENSTEK Data Center that require attention. To improve cyber security, we must overcome the major challenge of lack of training, awareness, and support from the top. We hope to improve cyber security at the ENSTEK Data Center by implementing the steps suggested by the participants, including increasing training, investing in advanced security technology, and conducting periodic audits and monitoring. Strict policies and heightened awareness of cyber security are crucial measures to safeguard data and ICT systems from cyber threats. Commitment and support from superiors directly contribute to three core components, i.e., training and awareness, monitoring and auditing, and effectiveness. These elements illustrate their pivotal role in strengthening cybersecurity measures at the ENSTEK Data Center.

Main Results and Observations

We obtained the main results and observations in this study through in-depth interviews with five civil servants at the ENSTEK Data Center of the Ministry of Education Malaysia. We analyzed the results of these interviews using coding and thematic analysis methods to identify the main themes that emerged from the data. We have organized the main findings into coding and themes, and provided a detailed description of the formation of these themes.

Table 3: Coding And Thematic Analysis Methods

Coding	Themes
Less steady	Weaknesses in Cyber Security
Needs Improvement	
Monitoring	
Staff Training	
Budget shortage	Challenges in Addressing Cyber Threats
Advanced cyber attacks	
Technological developments	
Superior support	
Many procedures	
Periodic audits	Effectiveness of Existing Measures
Some are effective	
Need to improve	
Technology updates	
Lack of awareness	Lack of Cyber Security Awareness
Security policy	Importance of Cyber Security Policy
Need support	The need for support from superiors
Additional training	Recommendations for Improving Cyber Security
New technology investment	

Description of Theme and Coding

Weaknesses in Cyber Security

Coding reveals deficiencies in training, monitoring, and improving cyber security. Participants stated that cyber security at the ENSTEK Data Center is still lacking and needs a lot of

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033
improvement. Adequate staff training and regular monitoring are essential to ensuring effective cyber security. These deficiencies make cyber security in data centers weak and vulnerable to threats. Without addressing these weaknesses, the data center remains at high risk of breaches that could compromise sensitive educational data.

Challenges in Addressing Cyber Threats

The theme of lack of budget, increasingly sophisticated cyber-attacks, technological advancements, and lack of support from superiors emerges from the code. Participants emphasized that lack of budget made it difficult to invest in more sophisticated security technologies. In addition, increasingly sophisticated cyberattacks make efforts to maintain cyber security more challenging. Experts often overlook the crucial role of superior support in effectively addressing cyber threats. Overcoming these challenges is crucial for maintaining the integrity and security of educational data, which is vital for the smooth operation of educational institutions.

Effectiveness of Existing Measures

Coding forms this theme, revealing varying perspectives on the efficacy of current security measures. Some participants feel that these measures are effective, but some feel that there is still a lot of room for improvement. The effectiveness of existing security measures also depends on periodic audits and security technology updates. The effectiveness of existing security measures also depends on periodic audits and security technology updates. This demonstrates the need to constantly update and adapt the implemented measures to the latest cyber threats. Ensuring the effectiveness of these measures is essential for protecting educational data from potential cyberattacks.

Lack of Cyber Security Awareness

This theme emerges from coding, indicating a lack of awareness among staff about cyber security. Participants felt that the level of awareness about the importance of cyber security was still low. This makes it difficult to implement effective security measures. Therefore, cyber security awareness campaigns should be conducted more frequently to increase staff knowledge and understanding of cyber threats and preventive measures that can be taken. Raising awareness is key to fostering a culture of security within educational institutions, ensuring that all staff are vigilant and proactive in protecting data.

The Importance Of Cyber Security Policy

Coding forms this theme, emphasizing the importance of a strict and clear cyber security policy. All staff must follow the security policy to ensure effective cyber security, according to the participants. Following security policies is crucial for safeguarding data and ICT systems. A robust cyber security policy is fundamental to safeguarding educational data and maintaining the trust of stakeholders.

This theme is formed from coding that emphasizes the importance of a strict and clear cyber security policy. Participants stated that the security policy must be followed by all staff to ensure effective cyber security. Adherence to security policies is an important step in ensuring data and ICT systems are protected. A robust cyber security policy is fundamental to safeguarding educational data and maintaining the trust of stakeholders.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

The Need For Support From Superiors

This theme emerges from the code, highlighting the critical role of superior support in ensuring the effectiveness of cyber security measures. Participants felt that without this support, efforts to implement security measures would face many obstacles. The superiors must be more proactive in supporting cyber security efforts and provide a sufficient budget to implement the required measures. Support from superiors is critical for the successful implementation of security measures, ensuring that educational data is adequately protected.

Recommendations for Improving Cyber Security

The coding reveals the participants' suggestions for enhancing cyber security at the ENSTEK Data Center. Key recommendations include increasing cyber security training for staff and investing in more security technology. Enhancing training and technology investments are crucial steps to fortify the data center against evolving cyber threats.

The study identified some supporting evidence to bolster the main findings. One of the dialogues that show weaknesses in cyber security is, "Umm, I think cyber security here, ehhh, is still not strong. We can enhance our efforts significantly, particularly in the areas of monitoring and staff training. These dialogues show that there are deficiencies in training and monitoring which are important aspects of ensuring effective cyber security. Another participant stated, "Ehhh, I think we have a good system but, umm, need regular updates and audits to make sure everything is working properly." This shows that even if there is a robust cyber security system, without regular updates and audits, the system may not be able to function optimally. Regular updates and audits are essential to maintain the effectiveness of cyber security measures and adapt to new threats.

Several key themes emerged during the discussion of the main findings. The theme of weaknesses in cyber security indicates that there is a lack of adequate staff training, which leaves them less prepared to face cyber threats. Furthermore, a lack of monitoring and periodic audits contributes to this weakness. Participants emphasized that without adequate training, staff cannot handle cyberattacks effectively. Furthermore, the lack of top-level support adds to the challenges in dealing with cyber threats. Participants stated that often they did not get enough support from their superiors to implement the necessary safety measures. This can be seen from the dialogue, "Mmm, the main challenge is the lack of trained staff and, aaa, sometimes it's hard to get support from the superiors." Support from superiors is critical to ensuring that staff have the resources and backing required to implement effective security measures.

This study also discusses the effectiveness of existing security measures. Although some participants think the measures are effective, others think they can be improved. Participants suggested that security technology be constantly updated, and staff training be improved. Dialogues such as "Eh, in my opinion, mmm, the current measures are quite effective but need improvement, aaa, especially in terms of technology," indicate that there is a need for continuous improvement in existing security measures. Continuous improvement and adaptation of security measures are necessary to keep pace with the evolving nature of cyber threats.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

In addition, the findings on the lack of awareness about cyber security show that many staff still do not understand the importance of cyber security measures. Participants recommended conducting cyber security awareness campaigns more frequently to enhance staff understanding and awareness. Another significant theme is the importance of a strict and clear cyber security policy. All staff must update and adhere to security policies for effective cyber security, according to participants. Frequent awareness campaigns and clear policies are essential to foster a culture of security within the organization.

While most findings support weaknesses and challenges in cybersecurity management, there are also unexpected or contradictory findings. For example, some participants stated that the existing cyber security system is **adequate** enough and only needs periodic updates and audits. This is contrary to the views of some other participants who feel that the system is still weak and needs a lot of improvement. Dialogues like, "Ehhh, I think we have a good system but, umm, need periodic updates and audits to make sure everything is working properly," indicate that there is a difference of opinion about the current state of cyber security systems. Addressing these differing perspectives is important to develop a balanced and effective approach to cyber security.

The study's findings reveal several weaknesses in the cyber security management at the ENSTEK Data Center that require attention. These weaknesses include a lack of training and monitoring, a lack of support from superiors, and a lack of awareness of the importance of cyber security. Technological updates and increased staff training can enhance the effectiveness of existing security measures. By taking the suggested measures, it is hoped that cyber security at the ENSTEK Data Center can be improved, and data and ICT systems can be protected from cyber threats. Implementing these recommendations will not only enhance the security of the data center but also contribute to the overall resilience of the educational infrastructure. These findings provide important guidance for the next steps in improving cyber security in government data centers.

Conclusion

This study identified several key findings through in-depth interviews with five civil servants at the Malaysian Ministry of Education's ENSTEK Data Center. These findings provide an in-depth picture of the weaknesses in cyber security management, the challenges faced, as well as the effectiveness of existing security measures.

Key findings identified include deficiencies in cyber security training, a lack of periodic monitoring and audits, and a lack of support from superiors. Participants also noted that there is a lack of budget to invest in more sophisticated security technology, which makes it difficult to effectively maintain cyber security. Increasingly sophisticated cyberattacks are also a major challenge facing data centers. Several key themes emerged from the analysis of these findings. The theme of weaknesses in cyber security indicates that there is a lack of adequate staff training, which leaves them less prepared to face cyber threats. Lack of monitoring and periodic audits. In addition, the lack of support from the top adds to the challenges in dealing with cyber threats. Participants stated that often they did not get enough support from their superiors to implement the necessary safety measures.

This study also discusses the effectiveness of existing security measures. Although some participants think the measures are effective, others think they can be improved. The

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

effectiveness of existing security measures also depends on periodic audits and security technology updates. This indicates that we must constantly update and adapt our measures to the latest cyber threats.

The findings on the lack of awareness about cyber security show that many staff still do not understand the importance of cyber security measures. Participants recommended conducting cyber security awareness campaigns more frequently to enhance staff understanding and awareness. Another significant theme is the importance of a strict and clear cyber security policy. All staff must follow the security policy to ensure effective cyber security, participants emphasized. Regular updates are necessary to keep this policy up-to-date with the latest cyber threats. Following security policies is crucial for safeguarding data and ICT systems.

Support from the top is critical in ensuring the effectiveness of cyber security measures. Participants felt that without this support, efforts to implement security measures would face many obstacles. They suggested that the superiors be more proactive in supporting cyber security efforts and provide a sufficient budget to implement the necessary measures.

In order to contribute to this field, this study provides in-depth knowledge of the challenges and weaknesses in cyber security management in government data centers. We can use the findings of this study as a guide to design policies and more effective security measures. Furthermore, this study emphasizes the importance of cyber security training and awareness among staff in order to increase their preparedness for cyber threats.

This study also contributes to the understanding of the need for support from superiors and a sufficient budget to implement effective cyber security measures. By taking the suggested measures, such as increasing training, investing in advanced security technology, and holding periodic audits and monitoring, it is hoped that cyber security at the ENSTEK Data Center can be improved, and data and ICT systems can be protected from cyber threats.

The objective of this study is to identify factors that cause a lack of expertise among civil servants in managing and implementing ICT security protocols in the Data Center of the Ministry of Education Malaysia, as well as analyze the level of information security awareness (ISA) among staff. The study's findings have successfully achieved the objective by identifying critical factors that influence the lack of expertise and the impact of awareness on safety protocol compliance. This study successfully achieved its objective by identifying training and technical knowledge deficiencies as key factors in ICT security management. Furthermore, the study revealed a low level of information security awareness, which impacted adherence to security protocols.

This study contributes to a deeper understanding of ICT security challenges in the government sector, particularly in the Data Center of the Ministry of Education Malaysia. It offers suggestions for enhancing training and raising staff awareness about various aspects of ICT security. Future studies can concentrate on implementing intervention measures like continuous ICT security training programs and examining the impact these improvements have on the data center's overall performance.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

Overall, this study reveals the need to address several weaknesses in cyber security management to ensure the security and integrity of data in government data centers. We hope to implement efforts to maintain cyber security more effectively by increasing training, awareness, and support from superiors, and investing in more sophisticated security technology. These improvements are essential not only for protecting data but also for ensuring the smooth operation of educational services, which rely heavily on secure and reliable data management systems. This study provides important guidance for the next steps in improving cyber security in government data centers and contributes to the cyber security literature in the context of government data management. Implementing these recommendations will enhance the resilience of educational infrastructure, ultimately benefiting students, educators, and the broader community.

Acknowledgments

My infinite gratitude goes to my family, who always provided moral support and encouragement throughout this writing. I would also like to express my appreciation to Universiti Teknologi MARA (UiTM), which has provided all the facilities and academic support needed throughout my studies. I am grateful to all the lecturers, friends, and those who assisted me in writing this by offering guidance, advice, and valuable information. I greatly appreciate your service and will remember it for the rest of my life.

References

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

Anthony Anyanwu, Temidayo Olorunsogo, Temitayo Oluwaseun Abrahams, Odunayo Josephine Akindote, & Oluwatosin Reis. (2024). Data Confidentiality and Integrity: a Review of Accounting and Cybersecurity Controls in Superannuation Organizations. *Computer Science & IT Research Journal*, *5*(1), 237–253. https://doi.org/10.51594/csitrj.v5i1.735

Bolek, V., Romanová, A., & Korček, F. (2023). The Information Security Management Systems in E-Business. *Journal of Global Information Management*, *31*(1), 1–29. https://doi.org/10.4018/JGIM.316833

Bolger, C., Brummel, B., Aurigemma, S., Moore, T., & Baskin, M. (2023). *Information Security Awareness: Identifying Gaps in Current Measurement Tools*. *2014*, 1–9.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Daher, W. (2023). Saturation in Qualitative Educational Technology Research. *Education Sciences*, *13*(2), 1–14. https://doi.org/10.3390/educsci13020098

Dioubate, B. M., Norhayate, W. D. W. A., Fakhrul, Z., Fauzilah, S., Hilmi, M. F., & Lee Ooi Hai. (2023). The Role of Cybersecurity on the Performance of Malaysian Higher Education Institutions. *Jurnal Pengurusan*, *67*. https://doi.org/10.17576/pengurusan-2023-67-03

Dirin, A. (2023). A Security Framework for Increasing Data and Device Integrity in Internet of Things Systems. *Sensors*. https://doi.org/10.3390/s23177532

Hamdah, N. H., Udin, M. M., Rosli, N. S. M., Khamri, Z. I. M., & Hussain, A. A. (2024). Exploring Factors Contributing to the Erosion of Integrity Among Education Personnel

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

in Malaysia: A Case Study in Perlis. *International Journal of Religion*, *5*(9), 795–804. https://doi.org/10.61707/wr8q5037

Hazmi, N. R., Abrizah, A., & Idaya, A. M. K. Y. (2023). Research data governance activities for implementation in Malaysia research performing organizations: insights from data practitioners via Delphi study. *Malaysian Journal of Library and Information Science*, *28*(3), 37–60. https://doi.org/10.22452/mjlis.vol28no3.3

Indriyanto, E. (2023). The Role Of Information Technology In Increasing Audit Process Efficiency. *Jurnal Ekonomi*, *12*(04), 1441–1446. https://ejournal.seaninstitute.or.id/index.php/Ekonomi/article/view/3211

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability (Switzerland)*, *14*(3). https://doi.org/10.3390/su14031269

Lee, R., & Ariffin, A. S. (2021). Awareness of Ict Security Policy To Ensure Data Protection in Forestry Department Peninsular Malaysia. *Journal of Science, Technology and Innovation Policy*, *7*(2), 65–74. https://doi.org/10.11113/jostip.v7n2.93

Lee, R., Ariffin, A. S., Shammugam, I., Samy, G. N., Magalingam, P., Maarop, N., Perumal, S., Shanmugam, B., Nor Kamaliah Mohammad, &Norfariza Mohd Radzi, & Zuraidah Abdullah. (2021). Information security threats encountered by Malaysian public sector data centers. *Jurnal Kepimpinan Pendidikan*, *1*(April), 53–64. https://doi.org/10.11591/ijeecs.v21.i3.pp1820-1829

Lim, W. M. (2024). *What Is Qualitative Research ? An Overview and Guidelines*. https://doi.org/10.1177/14413582241264619

Maniam, J. N., & Singh, D. (2020). Towards Data Privacy and Security Framework in Big Data Governance. *International Journal of Software Engineering & Computer Systems (Ijsecs)*, *6*(1), 41–51.

Mtukushe, N., Onaolapo, A. K., Aluko, A., & Dorrell, D. G. (2023). Review of Cyberattack Implementation, Detection, and Mitigation Methods in Cyber-Physical Systems. *Energies*, *16*(13), 1–25. https://doi.org/10.3390/en16135206

Nadeem, M. W., Goh, H. G., Aun, Y., & Ponnusamy, V. (2023). Toward Secure Software-Defined Networks Using Machine Learning: A Review, Research Challenges, and Future Directions. *Computer Systems Science and Engineering*, *47*(2), 2201–2217. https://doi.org/10.32604/csse.2023.039893

Nor Kamaliah Mohammad, &Norfariza Mohd Radzi, & Zuraidah Abdullah. (2014). Aspek Keselamatan Dan Privasi Data Dalam Pengurusan Data Raya Ppd Di Negeri Terengganu. *Jurnal Kepimpinan Pendidikan*, *1*(April), 53–64.

Rani, S., Kataria, A., Kumar, S., & Karar, V. (2025). A new generation cyber-physical system: A comprehensive review from security perspective. *Computers and Security*, *148*(February 2024), 104095. https://doi.org/10.1016/j.cose.2024.104095

Rao, S. P., Chen, H. Y., & Aura, T. (2023). Threat modeling framework for mobile communication systems. *Computers and Security*, *125*. https://doi.org/10.1016/j.cose.2022.103047

Sharma, A., Chauhan, A. S., & Vishwakarma, A. (2023). An Overview of Implementation Strategies on Cyber Security. *2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET)*, 625–628. https://doi.org/10.1109/ICSEIET58677.2023.10303587

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume 6 Issue 22 (September 2024) PP. 482-501
DOI: 10.35631/IJMOE.622033

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

Xue, Q., Liu, Y.-J., Sun, Y., Wang, J., Li, Y., Feng, G., & Ma, S. (2023). Beam Management in Ultra-Dense mmWave Network via Federated Reinforcement Learning: An Intelligent and Secure Approach. *Ieee Transactions on Cognitive Communications and Networking*. https://doi.org/10.1109/tccn.2022.3215527