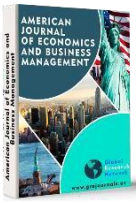

American Journal of Economics and Business Management

Vol. 7 Issue 12 | **pp. 1500-1509** | **ISSN:** 2576-5973

Available online @ https://www.globalresearchnetwork.us/index.php/ajebm

Article

Evaluating the Effectiveness of Accounting Information Systems in Enhancing Cybersecurity: A Case Study of Zain Iraq

Marwa Ridha Shakkur[1], Alaa Noora Khalaf[2]

1. University of Kirkuk
2. General Directorate of Education in Kirkuk Governorate

* Correspondence: marwaagha@uokirkuk.edu.iq

Abstract: In mild of rapid technological development and the growing reliance on virtual structures, cybersecurity has emerged as one of the most notable annoying conditions coping with corporations, specifically within the telecommunications place, which handles touchy monetary facts. This have a look at targets to assess the effectiveness of accounting facts structures in improving cybersecurity internal Zain Iraq, a main telecommunications organisation in Iraq. The studies is based at the hypothesis that accounting facts structures play a important position in protecting economic records and mitigating the risks of cyberattacks. Data were accumulated from a pattern of personnel operating in departments related to accounting facts systems and cybersecurity. The look at employed a questionnaire designed the usage of a 5-point Likert scale, alongside facet suitable statistical tools to check reliability, validity, and normal distribution of the results. The findings found out that accounting facts structures at Zain Iraq significantly make a contribution to enhancing cybersecurity via safeguarding monetary data, detecting suspicious sports, and regularly updating systems to cope with evolving threats. Continuous employee training at the solid use of the device become additionally determined to enhance the effectiveness of protection features. The study offers several pointers to beautify cybersecurity, such as strengthening safety updates, increasing employee education, and growing effective emergency reaction plans. This research gives treasured insights for telecommunications organizations aiming to construct more stable accounting systems, thereby enhancing employer stability and protecting touchy data towards developing threats.

Keywords: Evaluation, Effectiveness, Accounting Information Systems, Cybersecurity, Zain Iraq

Citation: Marwa Ridha Shakkur. Evaluating the Effectiveness of Accounting Information Systems in Enhancing Cybersecurity: A Case Study of Zain Iraq. American Journal of Economics and Business Management 2024, 7(12), 1500-1509.

Received: 10th Sep 2024
Revised: 11th Oct 2024
Accepted: 24th Nov 2024
Published: 27th Des 2024

1. Introduction

Amid the fast technological improvements and growing dependence on digital structures, cybersecurity has grow to be one of the most vital demanding situations for agencies throughout diverse sectors, especially in telecommunications. Accounting information systems play a critical characteristic in managing and protecting monetary information in the direction of cyber threats. This research makes a speciality of inspecting the effectiveness of accounting statistics structures in enhancing cybersecurity at Zain Iraq, one most of the most crucial telecommunications organizations within the united states of the usa.

Research Problem:

The research problem lies inside the developing cyber threats focused on financial facts and touchy records in telecommunications agencies. This necessitates evaluating the effectiveness of accounting records structures in presenting the required safety. The research trouble may be summarized within the principal question:

How effective are accounting information structures in enhancing cybersecurity at Zain Iraq?

Research Importance:

The significance of this research lies in the following factors:

1. Highlighting the position of accounting statistics systems in reaching cybersecurity.
2. Providing practical insights into the country of cybersecurity in Iraq's telecommunications zone.
3. Three. Contributing to the development of effective techniques to decorate cybersecurity in agencies.
4. Offering actionable pointers to improve the overall performance of accounting information structures inside the field of cybersecurity.

Research Hypothesis:

The examine is primarily based on the main speculation:

Accounting records structures appreciably make a contribution to enhancing cybersecurity at Zain Iraq.

This hypothesis can be divided into the following sub-hypotheses:

1. Accounting data structures provide adequate protection for monetary statistics against cyberattacks.
2. Accounting data systems are regularly up to date to counter evolving cyber threats.
3. Accounting data systems improve the organisation's capacity to hit upon and cope with suspicious activities.

Research Population and Sample:

The research population comprises all employees in the financial, accounting, and IT departments at Zain Iraq. The research sample includes a selected group of employees from these departments, considering diversity in job levels and practical experience. A stratified random sample will be used to ensure appropriate representation of various employee categories.

This research adopts a descriptive-analytical approach, utilizing a structured questionnaire directed at employees in relevant departments to measure their perceptions of the effectiveness of accounting information systems in enhancing cybersecurity.

Definition of Accounting Information Systems (AIS):

Accounting Information Systems (AIS) are included structures designed to collect, store, and method monetary and accounting statistics inside corporations. These structures purpose to support economic decision-making through imparting accurate and reliable information about the organization's financial performance. AIS streamline accounting strategies, enhancing efficiency and minimizing human mistakes. **(Horgan,2015)**

Components of Accounting Information Systems:

AIS include numerous key components, which include: (Roberts,2018)

1. Hardware:

   Devices which includes computer systems and servers used for facts input, processing, and storage. Hardware is vital for providing users with get admission to to financial records.

2. Software:

   Accounting software like QuickBooks and SAP that aids in processing monetary information and making ready reports.

3. Data:

Financial information accrued and processed, which include transaction statistics, accounting statistics, and monetary reviews.

4. Procedures:

   Policies and methods defining how the system is used, which includes facts access and processing protocols.

5. People:

   Users interacting with the system, consisting of accountants, managers, and financial analysts.

Importance of Accounting Information Systems:

AIS are vital for several motives: (Abdullah,2020)

1. Improved Efficiency:

   Automates habitual tasks, simplifying accounting strategies and lowering human errors.

2. Accurate Reporting:

   Produces particular monetary reports reflecting the enterprise's monetary popularity, aiding informed decision-making.

3. Decision-Making Support:

   Provides vital facts that facilitates control make strategic decisions primarily based on reliable information.

4. Enhanced Internal Controls:

   Implements powerful measures for recording and processing records as it should be, minimizing financial dangers.

Functions of AIS:

AIS have three primary functions:(Bin Saeed,2021)

1. **Efficient Collection and Storage of Financial Data:** The system collects transaction data from source documents, records it in journals, and posts it to ledgers.
2. **Providing Information for Decision-Making:** Generates managerial reports and financial statements for executives and key decision-makers within the organization.
3. **Establishing Necessary Controls:** Implements controls to ensure the accurate recording and processing of data, guaranteeing the reliability of financial information.

Development of AIS:

The evolution of AIS has been significant. Initially relying on paper-based records and manual bookkeeping, AIS have shifted to electronic systems with advancements in technology. This transformation has improved the speed and accuracy of financial data processing, making AIS more efficient and effective.

Challenges Facing AIS:

Despite their benefits, AIS face several challenges: (Al-Bayati,2019)

1. **Data Security:**

   Protecting financial data is critical as organizations face cyber threats that may result in sensitive information breaches.

2. **Integration with Other Systems:**

   Integrating AIS with other organizational systems, such as Human Resource Management Systems (HRMS) or Supply Chain Management Systems (SCMS), can be challenging.

3. **Rapid Technological Changes:**

Organizations must regularly update their systems to keep pace with technological advancements and ensure optimal system performance.

4. **User Training:**

Effective use of AIS requires ongoing user training to maximize system efficiency and effectiveness.

Cyber security : Concept, Objectives, and Major Threats

Definition of Cybersecurity

Cybersecurity encompasses a set of practices and technologies aimed at safeguarding systems, networks, and software from digital attacks. It involves protecting sensitive data and ensuring the integrity of business operations. In an era of growing electronic threats, cybersecurity has become essential for safeguarding critical information for both individuals and organizations. "Cybersecurity is no longer a technological 'option', but a societal need.**(alisawi,el al :2023)**

Cybersecurity also includes a fundamental component that monitors and analyzes data traffic to identify legitimate activities and detect malicious ones, as well as determine the type of attack: the Intrusion Detection System (IDS**).(Abdulmajeed,2022)**

Objectives of Cybersecurity

The primary objectives of cybersecurity include:(Al-Hammadi,2022)

1. **Data Protection:**

Prevent unauthorized access to sensitive information, preserving data confidentiality.

2. **Data Integrity:**

Ensure that data is not altered without authorization, maintaining the accuracy and reliability of information.

3. **Data Availability:**

Guarantee continuous access to authorized information, ensuring business efficiency.

Major Cybersecurity Threats

Accounting information systems face several cybersecurity threats, such as: (Al-Mansouri,2021)

- **Malware:**
  Including viruses and Trojan horses that aim to steal data or disrupt systems.
- **Cyberattacks:**
  Such as ransomware attacks, which lead to data loss and expose organizations to financial and legal risks.

The Relationship Between Accounting Information Systems and Cybersecurity

Accounting Information Systems (AIS) significantly influence cybersecurity measures. The more advanced AIS become, the greater the need for robust security measures to protect them from cyber threats. This relationship can be summarized as follows: (Al-Ataouna,2020)

- **Enhanced Protection:**

  Advanced AIS require sophisticated security strategies to safeguard sensitive financial data.

- **System Integration:**

  AIS should be integrated with cybersecurity solutions to provide comprehensive protection against attacks.

- **Raising Security Awareness:**

  Users must understand the importance of cybersecurity in protecting financial information, fostering a culture of security within the organization.

Importance of Cybersecurity

Cybersecurity provides several benefits, including: (Al-Dabbagh,2022)

1. **Protection of Critical Assets:**
   Safeguards organizational infrastructure, systems, data, and intellectual property.
2. **Customer Data Privacy:**
   Ensures companies protect customer data from theft or misuse.
3. **Minimizing Business Disruptions:**
   Reduces the impact of cyber threats on business operations.
4. **Regulatory Compliance:**
   Helps organizations adhere to information security laws and regulations.

Overview of Zain Iraq and Its Importance in the Iraqi Telecommunications Market

Zain Iraq is one of the leading providers of mobile communication and data services in Iraq and a subsidiary of Zain Group, established in 1983. The company began operations in Iraq in 2003 under the name "MTC Atheer" and became part of Zain Group in 2007.

Organizational and Financial Structure of Zain Iraq

Zain Iraq operates with a flexible organizational structure that enables it to adapt to rapid changes in the telecommunications market. Its structure includes several key departments, such as:

- **Senior Management**
- **Operations Management**
- **Marketing Management**
- **Information Technology Management**

Each department has defined roles contributing to the company's strategic goals.

Financially, Zain Iraq is a market leader in terms of revenue and profit. According to financial reports, the company generated revenues of $5.03 billion in 2021, reflecting its success in attracting a large customer base and offering innovative services that meet market needs.

2. Materials and Methods

Type of Research

The research adopts a **descriptive-analytical approach**, utilizing a quantitative method by collecting and analyzing statistical data related to accounting information systems and cybersecurity.

Research Population and Sample

The research targets employees working in departments related to accounting information systems and cybersecurity within **Zain Iraq**, including:

- **Accounting Department employees.**
- **IT Department employees.**
- **Cybersecurity Department employees.**

Research Sample:

- A random sample of 150 employees will be selected from the total research population of 400 employees.
- The sample will include various job levels to ensure comprehensive and accurate representation.

Data Collection Tools

Questionnaires:

- Questionnaires are the primary tool for collecting quantitative data.
- The questions are based on a five-point Likert scale to measure participants' attitudes and opinions regarding the impact of accounting information systems on cybersecurity.

To apply validity and reliability measures, Cronbach's Alpha will be used to evaluate the internal consistency of the questionnaire based on a sample of 150 respondents from the research population.

Validity Testing

Validity measures the accuracy of the questionnaire in evaluating the intended variables. Common methods are used to test the validity of the questionnaire.

Reliability Testing

To determine reliability, **Cronbach's Alpha** will be utilized, a widely used method for assessing internal consistency in questionnaires. The calculation will be performed using SPSS software.

Table (1): Cronbach's Alpha Coefficients

Item	Cronbach's Alpha (if Item Deleted)
Question 1	0.853
Question 2	0.854
Question 3	0.855
Question 4	0.854
Question 5	0.856
Question 6	0.853
Question 7	0.855
Question 8	0.857
Question 9	0.852
Question 10	0.850

Table Discussion:

The values in the table indicate that all questions have a high reliability level, with Cronbach's Alpha coefficients ranging from 0.85 to 0.86 when each item is excluded. This demonstrates strong internal consistency and high reliability of the questionnaire, ensuring its capability to effectively measure the role of accounting information systems in enhancing cybersecurity.

The table also shows the impact of excluding each item on the overall reliability, aiding in the evaluation of each item's significance in maintaining the required consistency.

Data Analysis Methods

The researcher used appropriate statistical tools to analyze the quantitative data, such as SPSS software, for conducting statistical tests, analyzing frequencies, means, and standard deviations to assess the effectiveness of accounting information systems.

3. Result and Discussion

Demographic Distribution

Table 2: Demographic Distribution

Category	Number	Percentage (%)
Gender		
Male	80	53.3
Female	70	46.7
Age		
Below 25 years	30	20.0
25–34 years	45	30.0
35–44 years	37	25.0
45–54 years	22	15.0
55 years and above	16	10.0
Educational Qualification		
Diploma	33	22.0
Bachelor's Degree	57	38.0
Master's Degree	45	30.0
Doctorate	15	10.0
Work Experience		
Less than 3 years	38	25.0
3–5 years	45	30.0
6–10 years	37	25.0
More than 10 years	30	20.0

Discussion of Table 2:

1. **Gender**:
   Males constitute 53.3% of the sample, while females represent 46.7%. This balanced distribution ensures representation of perspectives from both genders regarding the effectiveness of accounting information systems (AIS) in enhancing cybersecurity.
2. **Age**:
   The largest age group in the sample is 25–34 years (30%), followed by 35–44 years (25%). The younger (below 25 years) and older (55 years and above) age groups are less represented, with percentages of 20% and 10%, respectively. This distribution indicates a balanced representation across age groups, with a noticeable concentration among younger employees, reflecting the increasing interest of younger generations in cybersecurity technologies.
3. **Educational Qualification**:
   Bachelor's degree holders form the largest group (38%), followed by those with a Master's degree (30%), Diploma holders (22%), and Doctorate holders (10%). This distribution highlights a strong presence of highly educated individuals who are more likely to understand the requirements of cybersecurity and information technology.
4. **Work Experience**:
   Work experience is distributed across different categories, with 30% having 3–5 years of experience and 25% with less than 3 years. Employees with longer experience (6–10 years and over 10 years) represent 25% and 20%, respectively, indicating a balance between newer and more experienced employees in the sample.

Discussion of Survey Results

Table 3: Evaluation of the Effectiveness of AIS in Enhancing Cybersecurity

Question	Percentage (%)	Mean	Standard Deviation
AIS in the company helps protect financial data from breaches.	87.5	4.1	0.8
AIS is regularly updated to improve cybersecurity.	85.0	4.0	0.9

AIS can detect suspicious activities related to cyber threats.	82.0	3.9	0.85
AIS uses modern techniques like encryption to protect data.	78.5	3.8	0.9
The company regularly trains employees on safe use of AIS.	80.0	3.7	1.0
AIS has helped reduce the number of cyberattacks on the company.	81.0	3.8	0.95
AIS improves control over financial data and protects it from unauthorized access.	84.0	3.9	0.8
Effective response plans for cyber breaches are in place in the AIS.	79.5	3.7	1.1
The security level of AIS is sufficient to protect sensitive information from attacks.	83.0	3.9	0.9
AIS in the company can counter emerging and evolving cyber threats.	86.0	4.0	0.85

Detailed Discussion of Results:

1. **Protection of Financial Data**:
   With 87.5% agreement, a high mean (4.1), and low standard deviation (0.8), participants strongly agree that AIS effectively safeguards financial data.
2. **Regular Updates**:
   The 85% settlement indicates recognition of the importance of regular updates for cybersecurity. However, the standard deviation of 0.9 indicates a few variant in responses, highlighting room for improvement in replace procedures.
3. **Detection of Suspicious Activities**:
   An 82% agreement and an average of 3.9 reflect confidence in AIS's ability to hit upon threats, though improvements ought to boom the effectiveness of such talents.
4. **Use of Encryption**:
   The 78.5% agreement indicates good enough use of encryption however famous capacity for development to cope with superior threats.
5. **Employee Training:**
   While 80% agreement suggests everyday schooling, the higher wellknown deviation (1.0) highlights disparities in schooling effectiveness throughout employees, emphasizing the need for standardized education protocols.
6. **Reduction of Cyberattacks:**
   An 81% agreement factors to the gadget's role in mitigating attacks, but ongoing efforts to enhance protection strategies are important.
7. **Data Control and Protection:**
   An 84% agreement underscores the gadget's effectiveness in controlling and safeguarding financial statistics.
8. **Response Plans for Breaches:**
   With 79.5% agreement and the very best preferred deviation (1.1), issues remain regarding the adequacy of response plans, necessitating revisions to make certain strong preparedness.
9. **Sufficiency of Security Levels:**
   The 83% agreement reflects agree with in AIS security degrees however additionally suggests opportunities to bolster protections against rising threats.
10. **Countering Evolving Threats:**
    The 86% agreement suggests confidence inside the machine's ability to evolve to new threats, with a need for continuous updates to hold this capacity.

Summary of Discussion:

The findings spotlight general pleasure with the effectiveness of AIS in improving cybersecurity. However, discrepancies in critiques regarding updates, training, and reaction plans point to areas requiring development to strengthen the organisation's cybersecurity resilience.

4. Conclusion

In conclusion, this have a look at highlights the significance of accounting statistics structures (AIS) in enhancing cybersecurity within Zain Iraq. Through the gathering and evaluation of facts thru questionnaires, the research presents a comprehensive photograph of the position of AIS in safeguarding sensitive monetary facts from cyber threats. The findings monitor that the organization's accounting machine demonstrates a excessive stage of reliability and displays worker delight with its effectiveness in ensuring information security. This reinforces the machine's potential to counteract threats and continuously update itself to deal with rising demanding situations.

Research Findings

- Effectiveness of AIS: The effects affirm that AIS drastically make a contribution to protective financial records from breaches.
- Continuous System Updates: Regular updates to AIS decorate protection tiers and adapt to evolving cyber threats.
- Role of AIS in Monitoring and Threat Detection: The findings indicate that the gadget has the functionality for early detection of suspicious sports, supporting shield the organisation from capability threats.
- Training and Awareness: Regular worker training at the safe use of AIS is vital to protection strategies. The effects show a very good level of cybersecurity attention among personnel.

Research Recommendations

- Enhancing Security Updates: It is recommended to continue updating AIS to deal with emerging threats, utilizing superior strategies inclusive of encryption.
- Expanding Employee Training: Investing in everyday schooling applications is vital to elevating security cognizance among body of workers for comprehensive safety.
- Improving Emergency Response Plans: Revising and updating reaction plans for cyber breaches are vital to ensure entire readiness in emergencies.

In summary, this studies represents an crucial step toward know-how the pivotal position of AIS in cybersecurity and affords insights to help corporations expand more powerful protection techniques.

REFERENCES

[1] Abdulmajeed, Inam Abdullah. Husien, Idress Mohammed. MLIDS22- IDS Design by Applying Hybrid CNN-LSTM Model on Mixed-Datasets. Informatica 46 (2022) 121–134.

[2] Hourigan, Susan. Accounting Information Systems: A Theoretical and Practical Introduction. Translated by using Abdul Monem Salama. 4th version. Cairo: University Publishing House, 2015.

[3] Roberts, Alan. Accounting Information Systems: An Integrated Approach. Translated by Abdullah Al-Anzi. Riyadh: Al-Mareekh Publishing House, 2018.

[4] Abdullah, Samer. Cybersecurity Management: Theory and Application. Riyadh: King Fahd National Library, 2020.

[5] Alisawi, Muthana. Hammood, Layth. Ghazi, Alaan, Al-Dawoodi, Aras. Cyber Security After COVID 19: A Review. International Conference on Innovations in Science, Hybrid Materials, and Vibration Analysis. Volume 2839, Issue 1 ,29 September 2023.

[6] Al-Atawneh, Mahmoud. "The Effectiveness of Accounting Information Systems in Managerial Decision-Making: An Applied Study on Private Sector Companies." Master's Thesis, Al-Azhar University, 2020.

[7] Al-Dabbagh, Zaid. "The Impact of Cybersecurity Systems on Corporate Performance in Iraq: A Case Study of Zain." Master's Thesis, University of Baghdad, 2022.

[8] Al-Amri, Nora. "The Effectiveness of Cybersecurity in Protecting Institutional Data: A Comparative Study between Banks and Telecommunications Companies." Ph.D. Dissertation, King Saud University, 2021.

[9] Zain Iraq. "Zain Strategy." Accessed October 20, 2024. https://www.zain.com/SR2022/ar/09-our-strategy-ar/

[10] Almaiah, M. A. (2024). Classification of Cybersecurity Threats, Vulnerabilities and Countermeasures in Database Systems. *Computers, Materials and Continua*, *81*(2), 3189–3220. https://doi.org/10.32604/cmc.2024.057673

[11] Chu, K. F. (2024). Multi-Agent Reinforcement Learning-Based Passenger Spoofing Attack on Mobility-as-a-Service. *IEEE Transactions on Dependable and Secure Computing*, *21*(6), 5565–5581. https://doi.org/10.1109/TDSC.2024.3379283

[12] Demek, K. C. (2024). Bridging the gap in talent: A framework for interdisciplinary research on autism spectrum disorder persons in accounting and information systems. *International Journal of Accounting Information Systems*, *55*. https://doi.org/10.1016/j.accinf.2024.100712

[13] Hamon, R. (2024). Three Challenges to Secure AI Systems in the Context of AI Regulations. *IEEE Access*, *12*, 61022–61035. https://doi.org/10.1109/ACCESS.2024.3391021

[14] Huy, P. Q. (2024). Sustainable Decision Making in The Time of Uncertainty: Does Moral Intelligence Make It Different? *Pacific Asia Journal of the Association for Information Systems*, *16*(1), 144–174. https://doi.org/10.17705/1pais.16108

[15] Kadhim, Y. A. (2025). Using Neural Network Techniques and Logistic Regression to Detect Earning Management in Iraqi Economic Units. *Studies in Systems, Decision and Control*, *555*, 203–214. https://doi.org/10.1007/978-3-031-67890-5_20

[16] Kaminska, N. (2024). Modeling ship cybersecurity using Markov chains: an educational approach. *CEUR Workshop Proceedings*, *3679*, 22–35.

[17] Mustafa, F. M. (2024). Strategies for Strengthening Security in Accounting Information Systems. *Journal of Ecohumanism*, *3*(5), 293–315. https://doi.org/10.62754/joe.v3i5.3902

[18] Natour, A. R. Al. (2024). The Role of Forensic Accounting Skills and CAATTs Application in Enhancing Firm's Cyber Resilience. *2nd International Conference on Cyber Resilience, ICCR 2024*. https://doi.org/10.1109/ICCR61006.2024.10532901

[19] Sharma, N. (2024). Maximizing the Benefits of Information Technology in Healthcare Finance and Accounting: A Quantitative Exploration of Organizational practices. *Journal of Commercial Biotechnology*, *29*(1), 102–113. https://doi.org/10.5912/jcb2217

[20] Wang, X. (2024). Dynamic Evolution of Financial Technology and Artificial Intelligence for Economy Based on Bayesian Algorithm in Cyber-Physical System. *Human-Centric Computing and Information Sciences*, *14*. https://doi.org/10.22967/HCIS.2024.14.066