FABA
Finance, Accounting and Business Analysis
ISSN: 2603-5324

Finance, Accounting and Business Analysis
Volume 7 Issue 2, 2025
http://faba.bg/
ISSN 2603-5324
DOI: https://doi.org/10.37075/FABA.2025.2.07

Assessing the readiness of Algerian port enterprises to secure accounting practices through cybersecurity protocols

Ali DJELLABA

Department of financial sciences and accounting, Chadli Benjedid University, El Tarf, Algeria

Info Articles

History Article:
Submitted 29 July 2025
Revised 29 October 2025
Accepted 2 November 2025

Keywords:
Cybersecurity, Data Privacy, Accounting Practices, Annaba Port enterprise.

JEL: M15, K24, M41

Abstract

Purpose: This study aims to conduct a cybersecurity readiness assessment of Algerian port enterprises, with a specific focus on the Port of Annaba, to enhance the security of its accounting practices. The assessment will be conducted by first establishing the current state of the port's cybersecurity protocols and then evaluating these against best practice standards. It also seeks to provide evidence-based recommendations for enhancing the resilience of these types of enterprises against cyber threats.

Design/Methodology/Approach: Owing to the nature of the subject, we adopted a qualitative interviews and exploratory approach in order to capture vulnerabilities and opportunities in detail.

Findings: The study underscore the necessity for accounting professionals to integrate robust cybersecurity protocols and data privacy strategies into their operations, thereby enhancing the overall integrity and reliability of financial reporting in a rapidly evolving digital environment. Development efforts have to integrate cybersecurity with accounting, rather treating them as two different domains, but rather as co-dependent frameworks of governance internal operational lapses and external vulnerabilities.

Practical Implications: This paper highlights the critical need for Algerian port enterprises to strengthen their cybersecurity protocols in accounting practices. By adopting these measures, organizations can protect the integrity of financial data while fostering trust among stakeholders, which may lead to increased investment and enhanced operational efficiency within the competitive maritime sector. Additionally, this research is crucial to advancing scientific knowledge about cybersecurity and can be used to support the identification of new directions for future research.

Originality/Value: While global studies have examined the technical issues of cybersecurity on accounting, there are no such studies that look into the problems of Algerian ports. In addition, most existing approaches do not combine cybersecurity with other business functions like risk and corporate governance. This study intends to fill these gaps by formulating relevant recommendations for Algerian port enterprises.

Paper Type: Research Paper.

* Address Correspondence:
E-mail:djellaba.ali@univ-eltarf.dz

INTRODUCTION

The world has opened up discussions on accounting and cybersecurity in one breath and the term 'cybersecurity' is becoming more popular in accounting. As accounting systems in enterprises become increasingly digitalized through cloud computing, AI, and other advanced technologies, they also become more vulnerable to cyber threats such as the possibility of system data manipulation, system intrusion, and in the worst-case scenario, business fraud becomes a high probability.

Such issues are also covered in the academic literature. For instance, Gordon et al. (2003) argue that sharing information about security breaches could achieve a greater level of cybersecurity and propose an attempt to lessen the danger by joining forces among competing entities. In such restricted regions like Algeria, shared knowledge could make a considerable difference. Gansler and Lucyshyn (2005) emphasise the importance of cybersecurity programmes to enterprises' success, highlighting their failure to achieve desired outcomes stemming from complicated risk evaluation and ever-changing threats. This is reminiscent of the case in Algerian enterprises that face stringent cyber threat evolution challenges requiring adaptable, robust, and agile countermeasures, which are not always easy to come by in lean resource settings. Apart from spending, Gordon and Loeb (2002) developed the Gordon–Loeb Model, which provides an economic rationale on how to define optimal investment levels in security. In the case of Algeria, this model might help local enterprises encourage more economically responsible expenditure towards security instead of excessive spending or not spending at all, which is easier with the financial constraints in the region. Also, Hausken (2006) elaborates that investments occur given a return higher than the average attack level or as per some formal regulatory demand, calling for greater governance and enforcement, which is still one of the many areas understudied in a lot of Algerian enterprises. From the auditing point of view, Steinbart et al. (2013, 2018) also analyse that having a positive interaction between the internal audit function and the information security unit tends to produce favourable results concerning security, which is crucial for port operations involving a high level of financial and data precision. Moreover, the emphasis on transparency is supported by Gordon et al. (2006) as well as Li et al. (2018), who discovered that cybersecurity leakage is linked to improved incident forecasting as well as confidence within the market. This means that Algerian enterprises would implement better communication practices internally and externally regarding their cybersecurity policies.

Even with the increase in the awareness of cybersecurity threats, most Algerian enterprises, and particularly those in the more sensitive industries such as ports, despite the growing reliance on digital accounting systems in organizations like port enterprises, the integration of robust cybersecurity measures remains a significant challenge. The port's accounting systems handle vast amounts of sensitive financial data, making them a prime target for cyberattacks. However, outdated infrastructure, limited awareness of cybersecurity best practices, and unclear regulatory frameworks expose the port to risks such as data breaches, fraud, and operational disruptions. This raises the critical question: To what extent are Algerian port enterprises prepared to effectively integrate cybersecurity protocols into their accounting practices in order to protect financial data, improve operational resilience, and maintain stakeholder trust?

LITERATURE REVIEW AND CONCEPTUAL FRAMEWORK

Digital transformation in accounting practices

Accounting practices are the ways in which entities implement policies for capturing, processing, and reporting business-derived financial information as per recognized accounting disciplines and standards. These practices include the technical and procedural details of how financial transactions are handled and recorded in an entity to enable alignment, openness, and comparability of financial information over time and across entities. Accounting practices evolve in response to changes in the economic environment and conditions, or due to technological or regulatory shifts. These dynamic factors make accounting a critical area for the financial management of any organization (Weygandt et al. 2020).The change in technology has caused a complete shift to occur in the world of accounting and bookkeeping, changing the way financial records are kept and how information flows within the business. This aims to improve the level of efficiency and precision as well as improve the quality of decisions made at every level of the organization. Parlak (2020) emphasized that the accounting practices are impacted by digital transformation, which includes memorizing, classifying, and summarizing financial statements, analyzing and discussing financial statements, establishing the system, and ensuring effective continuity of the system (Arief 2024). In this situation, it is necessary to reassess and

realign practices and procedures. Future accountants must also have adequate knowledge and skills in digital accounting education, which includes new data analysis techniques, technology-driven auditing, and a comprehensive understanding of blockchain technology. The accounting profession is being transformed by digital technologies such as cloud computing, IoT, AI, and machine learning during the era of digital transformation. Accountants are not expected to be replaced by these technologies, but rather, they will allow them to focus more on strategic tasks that require creativity and intellectual depth. Future accountants must have the necessary analytical and strategic skills and be proficient in technology. Busulwa and Evans (2021) explain that the digital transformation of accounting practices is driven by both direct and indirect disruption.

Table 1. Digital disruption of accounting practices

Indirect disruption	direct disruption
- Changing the current most valuable accounting roles and activities. - Stakeholder expectations require accountants to perform new roles and activities in order to live up to these changed expectations. - The changes in accounting roles result in changes in the competencies required to fulfill these roles.	- Data availability. - The tools used to perform accounting work. - The type of value accountants are able to create. - The optimal ways to perform accounting work. - Competencies required by accountants.

Source: Busulwa and Evans (2021).

Digital transformation doesn't reduce the importance of accounting information, but it changes how stakeholders view the roles and tasks that accountants should undertake. It also influences their beliefs about how well accountants are fulfilling these roles to maximize the value of accounting. In this regard, digital transformation is, at least theoretically, a highly disruptive endeavor, focusing on fundamental transformations of both practices and products (Loonam et al. 2018).

The growing necessity of cybersecurity protocols in accounting practices

There are numerous definitions of cybersecurity, varying in emphasis but collectively pointing to the defence against digital threats. It is broadly defined as "a set of actions taken to defend against cyber-attacks and mitigate their consequences, including the implementation of necessary countermeasures." (Mamdouh Ibrahim 2023). From a functional perspective, cybersecurity can be defined as "the activity that ensures the protection of human and financial resources associated with information and communication technologies, minimising potential losses and enabling a swift recovery to prevent operational disruptions" (Bara 2017). Cybersecurity involves a comprehensive set of technical, organizational, and administrative practices aimed at protecting cyberspace from attacks. These include legal measures, data protection protocols, risk management strategies, and continuity planning to maintain system integrity, privacy, and functionality. The International Telecommunication Union, in its 2010–2011 telecommunication reform trends report, defined cybersecurity as "a set of tasks including tools, policies, procedures, guidelines, risk management strategies, training, best practices, and technologies to safeguard the cyber environment, organizational assets, and users" (ITU 2011). The American Institute of Certified Public Accountants stated that: "Cybersecurity is one of the top issues on the minds of executives and boards of nearly every company in the world—large and small, public and private" (Haapamäki and Sihvonen 2019).

It is important to distinguish between cybersecurity and information security. The former addresses all threats within cyberspace, whereas the latter focuses on protecting physical information assets. Therefore, cybersecurity is the broader concept. It interlinked with several core concepts (Mostafa 2008):

- **Cyberspace:** Defined by the French Agency for Information Systems Security (ANSSI) as "the communication space formed by the global interconnection of automated digital data processing equipment." It encompasses both physical and virtual components, including devices, software, networks, and users.
- **Cyberattacks:** These refer to "any action that disrupts or manipulates the functioning of a computer network, often exploiting system vulnerabilities to achieve national, political, or financial objectives."
- **Cybercrime:** Defined as "illegal acts carried out using digital equipment, systems, or the Internet," including criminal behaviour associated with data theft, network breaches, and exploitation via social networks.

In this context, accounting data has emerged as one of the primary assets that businesses use for value

chain analysis, strategic moves, and compliance checks. Whether compliance is legal, internal, or external. Nevertheless, this information encounters growing risks from criminal activity and cyber warfare. Cybersecurity relates to the magnitude of control exercised to protect computer systems with regard to maintaining the secrecy, wholeness, and accessibility of accounting information. Consequently, the impact of cyber security on accounting information quality has grown to become a major area of concern, particularly with digital infrastructure (Romney and Steinbart 2020).Accounting information is characterised by its dependability, precision, and impact for different parties, both internal and external, who use the information. The aforementioned characteristics are dependent on certain factors like accounting restatements that involve conflicts, transparency, substantiality verification, timely publication, availability of information, forgiving policies, and easy access through published works. As of yet, there is no unified definition of cybersecurity, it may be described as a combination of policies, professed actions, set rules, assigned specific roles, practised drills, associated procedures and infrastructures pertinent for safeguarding computer networks, systems, and databases from any unauthorised intrusion, tampering, cancellation, or wilful destruction (AICPA 2018).In terms of maintaining data confidentiality, cybersecurity helps maintain confidential accounting data and protects against unsolicited information and data leakage. This brings credibility when accounting information is given. A breach of accounting data might put its quality in danger. Strong security measures applied by the enterprise may safeguard them from forgers and undermine their data's accuracy. As for keeping data within reach, cybersecurity protects the system from a DDoS attack, which allows continuous information flow to be available uninterrupted. Also, following hypothetical regulation, protecting data under cybersecurity highly assists enterprises under stipulated region-bound laws and policies, which support the overall credibility alongside the quality of an enterprise's financial reporting (Romney and Steinbart 2020).In contrast, weak cybersecurity can lead to alteration of data which artificially generates accounting data that may not be true. Cyber records, which are very crucial when making decisions, like accounting records, can also be hacked and thus mailed, rendering them useless. Therefore, gaps in security pose investors and business partners having less trust in the financial accounts provided become easy. As is well-known, data sets to be recovered after a strange attack are always prone to payment hikes for system advancement or asset protection, as tactics aimed at improving cybersecurity together with the quality of accounting information and shielding accounting data from being received using data encryption technology (Whitman and Mattord 2022).However, a company cannot afford to fall behind its competitors in coming up with an effective cybersecurity strategy; it is not an option anymore but a vital strategic prerequisite. It is crucial to safeguard systems and information due to the risks associated with digital transformations.

A solid understanding of cybersecurity in the field of accounting is grounded in a number of well-established theories and models that outline effective ways to address and mitigate cyber threats. These frameworks offer essential conceptual guidance for developing robust cybersecurity strategies tailored to the financial sector. Important models of cybersecurity are outlined below:

Table 2. Models of cybersecurity

Model	Purpose	Accounting context	References
Defense-in-Depth (DiD)	The Defense-in-Depth model employs a layered security approach, implementing multiple protective measures across different organizational levels to secure financial information. This model operates on the premise that no single defense mechanism is entirely reliable; therefore, a combination of layers enhances overall protection against cyberattacks.	This includes safeguards such as physical security, network protocols, endpoint protection, encryption of data, and continuous system monitoring.	Shostack (2014)
Zero Trust	The Zero Trust model is built around the philosophy of "never trust, always verify." It requires rigorous identity verification	This model is especially pertinent to accounting firms, as it protects sensitive financial data by minimizing the risk of	Shore et al. (2021)

	and tight access controls, regardless of whether a user operates inside or outside the organization's network.	unauthorized access and internal breaches.	
Risk Management Framework (RMF)	Developed by the National Institute of Standards and Technology (NIST), the Risk Management Framework (RMF) provides a systematic method for identifying, analyzing, and managing cybersecurity risks.	This framework enables organizations, including accounting firms, to better understand their risk environment and apply appropriate security measures. It also assists in prioritizing cybersecurity investments based on the potential impact of various threats on financial information	NIST (2016)
Cybersecurity Maturity	The Cybersecurity Maturity Model measures an organization's cybersecurity performance across several critical areas, such as risk management, response to incidents, and continuous monitoring.	It enables accounting firms to assess their current security practices and pinpoint areas for improvement.	Rabii et al. (2020)
Principle of Least Privilege	The Principle of Least Privilege is a foundational cybersecurity concept that limits user access to only the data and systems necessary for their roles. This approach helps prevent unauthorized access to sensitive financial information and minimizes the impact of insider threats	When applied effectively in accounting settings, it ensures that employees handle only the information relevant to their responsibilities, thereby strengthening data security.	Saltzer (1975)

Source: Derived from a literature review by researcher.

Data protection in the face of digital threats

The transmission of data across networks that lack robust security measures poses serious risks to privacy and confidentiality. Sensitive communications, such as emails, can be intercepted and read by unauthorised parties, while personal and organizational data files may be illegally accessed. These vulnerabilities highlight growing concerns about privacy violations, particularly as the number of internet users and individuals' interacting with information systems continues to rise. This situation necessitates an examination of the measures implemented to safeguard data against such threats.

The United Nations has made substantial efforts to safeguard private life against technological advancement and protect individuals and their liberties from violation. These endeavors culminated in the inaugural International Conference on Human Rights, convened in Tehran in 1968. The conference emphasized that electronic computers represent the most significant threat to privacy and personal liberty, as they serve as modern surveillance instruments and spying tools. When personal information is stored on computers and examined, it discloses patterns of interaction and connections (UN 1968). Germany was actually the first country to introduce a legal framework for data privacy, starting with a state law in Hessen back in 1970. Then in 1977, Germany passed a national data protection law. Other countries quickly followed: Sweden created a similar law in 1973, and France passed its well-known "Information and Freedoms" law in 1978 (Mustafa 2016). Canada has also passed a privacy law that includes ten key principles for protecting personal information online (Al-Shawabkeh 2009). Similar protections exist in China, Austria, and Belgium. In Tunisia, lawmakers responded to digital advancements by including data protection rules in their 2000 Electronic Commerce Law, followed by a dedicated Personal Data Protection Law in 2004.

At the regional level, the Council of Europe has assumed a vital role. The Council of Europe Convention on the Protection of Individuals against the Hazards of Automated Processing of Personal Data was signed and became effective in October 1958 (Al-Shawabkeh 2009).Moreover, the Council has issued several recommendations to broaden protection, most notably Recommendation No. 13/R80 in 1980 concerning the exchange of legal data related to data protection. OECD has also played a key role. The OECD guidelines on privacy protection and Transborder data flows are recognized efforts in this context (OECD 2022).The General Data Protection Regulation (GDPR) is the European Union's all-encompassing framework for securing personal data. It seeks to enhance individuals' rights to manage their personal information and encourage clarity in its acquisition and use (GDPR 2025). Additionally, the African Union Convention on Cybersecurity and Personal Data Protection of 2014 guarantees the right to the integrity of personal data.

Besides the international and regional efforts to protect personal data, many countries and international organizations have created their own laws to deal with this issue. In Algeria, lawmakers passed Law 18-07, which focuses on protecting individuals when their personal data is being processed. The Algerian legislator provides a comprehensive legal definition in Article 3 of Law 18-07, characterising personal data as "any information, regardless of its basis, related to an identified or identifiable natural person (termed the data subject), whether directly or indirectly through reference to an identification number or one/multiple elements pertaining to their physical, physiological, genetic, biometric, psychological, economic, cultural or social identity." The same legal provision defines the data subject as any natural person whose personal data undergoes processing. Furthermore, the law establishes that personal data processing constitutes "any operation or set of operations performed with or without automated means on personal data, including collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, communication through transmission or publication, alignment, interconnection, blocking, encryption, deletion or destruction." Some legal interpretations specifically define automated processing as encompassing any process or series of processes (automated or manual) applied to personal data, covering collection, recording, structuring, preservation, modification, extraction access, utilisation, transmission, dissemination or any other form of making information available.

This law was an important step forward, especially because it introduced the principle of prior consent, meaning no one's data can be used without their clear and direct permission. To make sure the law is respected, Algeria set up a body called the National Authority for the Protection of Personal Data. Its job is to ensure that the use of modern technology doesn't threaten people's rights, freedoms, or private lives.

RESEARCH METHODOLOGY

Research Design

The study follows a case study design using Annaba port enterprise as a representative example of the cybersecurity concerns in Algerian ports. This approach has been possible because of the methodological freedom available in case studies which permits collection of rich data about the phenomenon of interest within the context in which it arises.

Instrument construction

The interview is the most appropriate tool for exploring this topic because it provides detailed insights into the phenomenon. The interview plans, which include three sections, were created based on existing research and adjusted to fit the current context in Algeria, and then it was presented to arbitration for revision (Appendix1).

Data collection methods

The research utilises a variety of primary and secondary data sources:

- **Primary Data:** The study evaluated the level of awareness of cybersecurity threats, system vulnerabilities, and gaps in compliance among IT and accounting personnel through interviews and direct structured observations "data for methodological triangulation."
- **Secondary Data:** The study has relied significantly on available literature, including government documents, textbooks, and peer-reviewed articles (for example, Law 18-07 on the protection of personal data, and international standards like the GDPR, ISO/IEC 27001, and AICPA's trust services framework).

Research scope

Annaba Port Enterprise was selected as a representative case study due to its similar state-owned structure and regulatory environment shared with Algeria's other major commercial ports, focusing on the integration of accounting systems with cybersecurity protocols. It does not discuss the IT infrastructure's topology, rather its relevance to the security and integrity of accounting information.

Analytical framework

In interrogating the gathered data, a thematic content analysis approach was adopted. This included:

- Coding data based on confidentiality, system vulnerabilities vis-a-vis data consciousness sophistication, and compliance to regulation as guided by law themes;
- Tracking implementation gaps between cybersecurity and qualitative indicators of accounting information systems (e.g. reliance, precision, comprehensiveness: timeliness);
- Examining data from Annaba Port against global standards.

RESULT AND DISCUSSION

At Annaba Port Enterprise, accounting is much more than compliance with laws and regulations; it is the key enabler of operational effectiveness and fostering trust among stakeholders. Well-kept financial records allow the port to effectively manage resources, eliminate unnecessary spending, and streamline processes. The ability to see accounts helps the credibility of the stakeholders, while the reliable accounting data smoothens the audits, lowering the chances of incurring fines or getting embroiled in legal issues. Like all other Algerian port enterprises, this port also uses digital technology, which in itself poses a threat of cyberattacks. Such breaches can interfere with company operations, expose confidential information, or alter financial statements, all of which can severely impair the organization.

The results presented below are derived from a methodologically triangulated approach. This approach relied on direct structured observations of specific accounting and security protocols, complemented by structured interviews conducted with a sample of 16 senior employees from the financial and accounting departments at the Annaba Port enterprise. This combined evidence base provided both the self-reported data and observed practice, yielding the following findings:

Table 3. Interview results

Axis	Dimension	Results
Training and cybersecurity awareness	information security training	Only 7 employees (43.75%) reported receiving training on how to secure systems and networks, while 9 employees (56.25%) had not received any such training.
	awareness of cyber risks	10 employees (62.5%) stated that they are aware of the risks associated with using open networks and unsafe software. On the other hand, only 3 employees (18.75%) admitted to being unaware of these risks.
	adherence to security procedures	11 employees (68.75%) acknowledged personally following the enterprise's security procedures. Meanwhile, 5 employees (31.25%) did not adhere to these procedures.
	human error	All participants (100%) agreed that human error is one of the main challenges in protecting data within the internal network of the organization.
Technical infrastructure	information systems	10 employees (62.5%) confirmed that the enterprise uses modern systems equipped with encryption and authentication. However, 6 employees (37.5%) disagreed.
	internal network protection	8 employees (50%) stated that the internal network is secured with a firewall and anti-intrusion software. In contrast, 5 employees (31.25%) said otherwise.
	data backup	All participants (100%) reported that regular backups of the accounting system’s data are performed.
	access control	14 employees (87.5%) confirmed the existence of a system that controls access permissions. Only 2 employees (12.5%)

Axis	Dimension	Results
		did not observe such a system.
Legal and regulatory framework	existence of national legislation	11 employees (68.75%) confirmed the existence of national legislation to protect systems. 5 employees (31.25%) remained neutral.
	compliance with legislation	12 employees (75%) reported that the enterprise complies with regulations related to digital data protection. Only 1 employee (6.25%) denied this, while 3 employees (18.75%) were neutral.
	internal guidelines	10 employees (62.5%) confirmed the presence of clear internal instructions for handling cyber incidents. 3 employees (18.75%) denied the existence of such guidelines, and another 3 were neutral.
	legal actions	13 employees (81.25%) indicated that legal measures are taken in case of a breach, while 3 employees (18.75%) remained neutral.

Source: Data processed from observations and interviews (Q2 2025).

The data shows that while the enterprise makes efforts to train employees in cybersecurity, the level of actual implementation of this training varies. A majority of respondents indicated they had received some form of cybersecurity training, yet a notable portion remained neutral or stated otherwise, which points to inconsistency in training coverage. Awareness of cyber risks is relatively high, but there are still gaps, particularly concerning risky behaviours such as the use of open networks or unverified software. This leaves them open to phishing, social engineering, and even inadvertent data breaches. There were no routine training sessions or mock exercises conducted. Furthermore, while many employees report adhering to security protocols, human error continues to pose the most significant threat to information system protection, as acknowledged unanimously by the respondents.

The results suggest that the enterprise uses moderately up-to-date information systems, protected by encryption, authentication tools, and internal firewalls. However, there is still room for improvement, especially in areas such as backup frequency and more precise control over access permissions. The existence of access control systems is a positive indicator, yet it must be supported by periodic audits and stricter implementation protocols to minimize vulnerabilities. In addition to the threats of keeping data private, the port enterprise does not have basic encryption policies, protocols, or measures on ports and interdepartmental communication for sensitive financial documents. This puts at risk the confidentiality of financial reports; they may be leaked and/or tampered with by some third parties. As for data availability, some reports noted that the downtimes of the system have severely affected the accessibility to the accounting data during the month-end reporting and financial review periods. This poses a major concern to availability, which forms part of the CIA Triad alongside confidentiality, integrity, and availability.

There is a generally favorable response regarding compliance with national regulations for information system protection. Most respondents confirmed the presence of national legislation and the enterprise's adherence to it. However, internal protocols for handling cybersecurity incidents are still underdeveloped according to a portion of participants. Legal action appears to be taken in the event of a breach, which is strength, but the extent to which these measures are effectively applied remains uncertain and would benefit from regular review and updates. The port also currently sits outside the compliance area of international cybersecurity frameworks of GDPR and ISO/IEC 27001. This puts the port in risky position legally in future international collaborations while damaging its reputation concerning financial reporting. It is important to note that the underlying principles and assessed controls, such as perimeter defense, access management, and incident response, are fundamental security mechanisms and are thus relevant for protecting other sensitive systems within the port, including operational and administrative data.

The SWOT analysis provides a strategic evaluation of Annaba Port Enterprise's cybersecurity readiness, particularly in relation to its human resources, technical infrastructure, and organizational procedures. It identifies the internal strengths and weaknesses of the enterprise, as well as the external opportunities and threats that may impact its ability to effectively protect its information system. This analysis serves as a tool to guide future improvements and decision-making in cybersecurity strategy and organizational resilience.

Table 4.SWOT Analysis

Strengths	Weaknesses
A majority of employees (62.5%) are aware of cyber risks.	Over half of the staff (56.25%) has not received formal training in information security.
High level of adherence to security procedures (68.75%).	Not all employees are aware of internal cybersecurity guidelines.
Regular data backups are consistently performed (100%).	Some employees (37.5%) believe the IT systems lack sufficient protection.
Access control systems are implemented (87.5%).	Presence of human errors is unanimously seen as a major risk.
Opportunities	**Threats**
Possibility to implement structured training programs to improve cybersecurity skills.	Cyber threats are becoming more complex and frequent.
National laws support the enterprise's legal framework for cybersecurity.	Lack of training may lead to exploitable human vulnerabilities.
Investments in advanced firewalls and encryption systems can enhance protection.	Over-reliance on technical infrastructure without ongoing human awareness.
Increasing international focus on port cybersecurity can open funding and support opportunities.	Internal network breaches can result in severe operational and reputational damage.

Source: Derived from interview results by researcher.

Based on the interview results and subsequent analysis, it is evident that the Annaba Port enterprise has made considerable efforts toward securing its information system. These efforts include investing in a relatively modern technical infrastructure and attempting to raise staff awareness regarding cybersecurity measures. However, the increasing and evolving nature of cyber threats demands continuous improvement and regular evaluation of readiness, particularly concerning employee training, reduction of human error, and stronger enforcement of internal cybersecurity protocols.

It should also be noted that while the Annaba Port enterprise is considered contextually representative of the cybersecurity concerns across the ten Algerian port enterprises—given the uniformity of mandatory cybersecurity measures implemented nationwide—it is essential to note the inherent limitations to generalizability. The findings of this single-site case study are best interpreted as context-specific insights and may not be generalizable across the entire national port system without further corroboration.

SUGGESTIONS AND RECOMMENDATIONS

Based on the theoretical insights and practical findings of this study, the following recommendations are proposed to strengthen the cybersecurity posture of Algerian port enterprises and improve the quality of their accounting information systems:

1. **Enhance employee training and awareness**
- Conduct regular cybersecurity training sessions for all accounting and IT personnel
- Simulate phishing attacks and provide feedback to reduce human error risks
- Distribute clear and concise security guidelines to all staff

2. **Modernize the technical infrastructure**
- Upgrade outdated accounting systems with modern platforms that include built-in encryption, access control, and audit logs
- Implement multi-factor authentication (MFA) for all financial system users
- Regularly update firewalls, antivirus, and anti-intrusion systems

3. **Strengthen regulatory compliance**
- Align internal data protection practices with international standards such as GDPR and ISO/IEC 27001
- Appoint a compliance officer or data protection officer (DPO) to monitor implementation

- Conduct periodic audits to ensure adherence to Law 18-07 and other national regulations

4. **Improve internal cybersecurity policies**

- Develop a formal incident response plan that clearly defines roles, procedures, and reporting timelines
- Establish clear protocols for system access, data classification, and incident escalation
- Apply the "Principle of Least Privilege" to restrict access to sensitive financial data

5. **Conduct regular risk assessments**

- Perform vulnerability assessments and penetration testing at least annually
- Use the cybersecurity maturity model to track progress and identify gaps
- Integrate risk assessment results into strategic and operational planning

6. **Promote a culture of cybersecurity**

- Include cybersecurity performance in employee evaluations and departmental KPIs
- Encourage management to lead by example in adhering to digital best practices
- Communicate regularly about ongoing threats, lessons learned, and system updates

7. **Leverage strategic partnerships**

- Collaborate with national and international cybersecurity agencies for training and threat intelligence
- Explore partnerships with universities or research centers to benefit from up-to-date expertise and solutions

CONCLUSION

This study has explored the critical intersection between cybersecurity and accounting practices, and evaluating the readiness of the Algerian port enterprises, which are a vital gateway in Algeria's economic infrastructure. As digital transformation expands the scope and complexity of accounting systems, the need to secure these systems against cyber threats becomes not only a technical imperative but a strategic necessity. Investing in cybersecurity as in the case with Algerian port enterprises means also investing in reliability of the accounts, operational efficiencies, and the public's trust in the system. Development efforts have to integrate cybersecurity protocols with accounting, rather than treating them as two different domains, but rather as co-dependent frameworks of governance internal operational lapses and external vulnerabilities.

While this research provides valuable insights into the role of cybersecurity in protecting accounting information systems within Annaba Port Enterprise, several avenues remain open for further exploration:

- Comparative Case Studies: Future research could look at more than one Algerian port enterprise or other important infrastructure organizations to see how their cybersecurity maturity and accounting system integration differ;
- Quantitative impact analysis: A more data-driven study could evaluate the direct financial impact of cybersecurity investments on the accuracy and timeliness of accounting reports or audit outcomes;
- Longitudinal studies: Over time, keeping an eye on how Annaba Port Enterprise's cybersecurity measures are being used could show patterns, improvements, or new problems that static studies cannot capture;
- A more in-depth look at human factors: Future work could focus more deeply on the human element by studying employee behaviour, resistance to change, and the effectiveness of different training methods;
- Development of a cybersecurity readiness index: A customized evaluation tool could be created to measure and benchmark the cybersecurity readiness of accounting systems in Algerian enterprises, helping guide policy and investment decisions;
- Exploration of AI and blockchain applications: With the increasing integration of artificial intelligence and blockchain in accounting, future studies could explore how these technologies may enhance cybersecurity and data protection in financial operations.

REFERENCES

Abu-Musa, A. A. 2006. Perceived security threats of computerized accounting information systems in the Egyptian banking industry, *Journal of Information Systems* 20 (1): 187–203. https://doi.org/10.2308/jis.2006.20.1.187.

AICPA. 2018. Why use the AICPA's cybersecurity risk management reporting framework. https://www.aicpa-cima.com/resources/download/why-use-the-aicpas-cybersecurity-risk-management-reporting-framework.

Al-Shawabkeh, M. A. 2009. *Computer and Internet Crimes*, 1st Ed. Amman: Dar Al-Thaqafa for Publishing and Distribution.

Arief, S. 2024. 'Digital transformation in accounting: the nexus between technology, leadership, and beyond'. In: Arif, P., and Tawei, W. (Ed.), *Digital Transformation in Accounting and Auditing*, Springer Books, 29-59.

Bara, Samir. 2017. Cybersecurity in Algeria: Policies and Institutions, *Algerian Journal of Human Security* 2 (2): 255-280.

Busulwa, R., and N. Evans. 2021. *Digital transformation in accounting*. 1st Ed. London-New York: Routledge.

EU. 2016. General data protection regulation GDPR, Official journal of the European Union. https://gdpr-info.eu/.

Gansler, J. S., and W. Lucyshyn. 2005. Improving the security of financial management systems: What are we to do?, *Journal of Accounting and Public Policy* 24 (1): 1-9. https://doi.org/10.1016/j.jaccpubpol.2004.12.001.

Gordon, L. A., and M. P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security* 5 (4): 438-457. https://doi.org/10.1145/581271.581274.

Gordon, L. A., M. P. Loeb, and W. Lucyshyn. 2003. Sharing information on computer systems security: an economic analysis. *Journal of Accounting and Public Policy*, 22: 461-485. http://dx.doi.org/10.1016/j.jaccpubpol.2003.09.001.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and T. Sohail. 2006. The impact of the Sarbanes-Oxley act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, 25: 503-530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005.

Haapamäki, E., and J. Sihvonen. 2019. Cybersecurity in accounting research, *Managerial Auditing Journal* 34 (7): 808-834. https://doi.org/10.1108/MAJ-09-2018-2004.

Hausken, K. 2006. Income, interdependence, and substitution effects affecting incentives for security investment, *Journal of Accounting and Public Policy,* 25(6): 629–665. https://doi.org/10.1016/j.jaccpubpol.2006.09.001.

ITU. 2011. Telecommunication reform trends: enabling tomorrow's digital world. https://www.itu.int/en/publications/ITU-D/pages/publications.aspx?pub=REGTR-2010-01.

Law 18-07 of June 10, 2018 on the protection of natural persons in the field of processing personal data, Algerian Official Journal No. 3.

Li H., W. G. No, and T. Wang. 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30: 40–55. https://doi.org/10.1016/j.accinf.2018.06.003.

Loonam J., S. Eaves, V. Kumar, and G. Parry. 2018. Towards digital transformation: Lessons learned from traditional organization. *Strategic Change*, 27 (2):101–109. https://doi.org/10.1002/jsc.2185.

Mamdouh Ibrahim, K. 2023. *Digital Judicial Expertise in Cybercrime (a comparative study in Egyptian, UAE and US law)*, 1st Ed, Alexandria: Dar Al- Fikr Al-Jami'i.

Mostafa, M.M. 2008. *Criminal Investigation in Cyber Crimes*, 1st Ed, Cairo: Police Press.

Mustafa, A. B. Q. 2016, *The right to information privacy between technical challenges and the reality of legal protection*, *Arab Journal of Science and Research Dissemination,* 2 (5):38-52.*https://doi.org/10.26389/AJSRP.A17316.*

NIST. 2016. NIST risk Management framework. https://csrc.nist.gov/projects/risk-management/about-rmf.

OECD.2022. OECD guidelines on the protection of privacy and transborder flows of personal data.https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html.

Rabii A., S. Assoul, T. K. Ouazzani, and O. Roudies. 2020. Information and cyber security maturity models: A Systematic Literature Review, *Information & Computer Security*, 28 (4): 627-644. https://doi.org/10.1108/ICS-03-2019-0039.

Romney, M. B., and P. J. Steinbart. 2018. *Accounting Information Systems*. 14th Ed. USA: Pearson Education.

Saltzer, J. H., and M. D. Schroeder. 1975. The protection of information in computer systems, Proceedings of the IEEE, 63(9): 1278-1308. https://doi.org/10.1109/PROC.1975.9939.

Shore M., S. Zeadally, and A. Keshariya. 2021. Zero Trust: The What, How, Why, and When. *Computer*, 54 (11): 26–35. https://ieeexplore.ieee.org/document/9585170.

Shostack, A.2014. *Threat Modeling: Designing for Security*, 1st Ed, USA: John Wiley & Sons.

Steinbart P. J., R. L. Raschke, G. Gal, and W. N. Dilla. 2013. Information security professionals' perceptions about the relationship between the information security and internal audit functions, *Journal of Information Systems*, 27(2): 65–86. https://doi.org/10.2308/isys-50510.

Steinbart, P. J., R. L. Raschke, G. Gal, and W.N. Dilla. 2018. The influence of a good relationship between the internal audit and information security functions on information security outcomes, *Accounting, Organizations and Society*, 71: 15–29.https://doi.org/10.1016/j.aos.2018.04.005.

UN. 1968. International conference on human rights, Tehran.https://www.un.org/en/conferences/human-rights/teheran1968.

Weygandt, J. J., P. D. Kimmel, and D. E. Kieso. 2020. *Accounting principles*. 14th Ed. Hoboken: John Wiley & Sons.

Whitman, M. E., and H. M. Mattord. 2022. *Principles of Information Security* .7th Ed. Boston: Cengage Learning.

APPENDIX 1. Interview plans

Section one: Human resource readiness in protecting the information system

This topic addresses the preparedness of human resources within the enterprise to face cybersecurity threats through their training and behaviour while interacting with systems and networks.

Statement	Yes	No	Comments /Clarifications
Do employees receive training on securing systems and networks from cybersecurity threats?	☐	☐	
Are employees aware of the risks associated with using open networks and insecure software?	☐	☐	
Do employees personally commit to following security procedures when using the information system?	☐	☐	
Are human errors considered one of the main challenges in protecting data over the internal network of the enterprise?	☐	☐	

Section two: Effectiveness of technical infrastructure (systems and networks)

This topic focuses on the effectiveness of the technical infrastructure, including information systems and internal communication networks, and their ability to defend against cybersecurity attacks.

Statement	Yes	No	Comments / Clarifications
Does the enterprise rely on modern information systems protected by multiple encryption and authentication technologies?	☐	☐	
Is the internal network protected by firewall and intrusion detection software?	☐	☐	
Is regular data backup conducted for the accounting system to prevent data loss?	☐	☐	
Is access to the information system controlled through specific accounts and monitored?	☐	☐	

Section three: Legal and regulatory framework for cybersecurity

This topic addresses the existence of legal and regulatory frameworks that govern and guide the protection of information systems and networks from cybersecurity attacks within the enterprise.

Statement	Yes	No	Comments / Clarifications
Are there national legal provisions regulating the protection of systems and networks against cyberattacks?	☐	☐	
Does the enterprise comply with regulations regarding the protection of digital data and electronic accounting transactions?	☐	☐	
Are there clear internal guidelines for handling hacking incidents or data breaches?	☐	☐	
Are legal actions taken in case of a breach or violation of systems?	☐	☐	