**Ziglôbitha,**
Revue des **A**rts, **L**inguistique,
**L**ittérature & **C**ivilisations
Université Peleforo Gon Coulibaly - Korhogo

# Strengthening Cybersecurity of Public Accounting Data in Algeria: A Comparative Analysis of Gaps and Challenges with Developed Countries

**BENDOUKHA Mohammed Reda**
[1] Economic and Local Development Studies Laboratory in the Southwestern Region University of Tahri Mohamed Bechar,
redamedreda3129@gmail.com
ORCID: 0000-0002-3967-127X

**BOUFELDJA Kalloum**
[2] Economic and Local Development Studies Laboratory in the Southwestern Region University of Tahri Mohamed Bechar,
boufeldjak8@gmail.com
ORCID: 0009-0002-6981-3803

**Abstract:** The study revealed that accounting data faces numerous threats, including viruses, ransomware attacks, and cyber fraud, which compromise data accuracy and reliability. Compared to developed nations like the United States and Germany, Algeria lags in cybersecurity due to inadequate technical infrastructure, a shortage of specialized personnel, and weak legislation and security policies. Using a comparative analytical approach, the study assessed cybersecurity levels in Algeria versus developed countries, identifying key gaps and challenges. The findings underscored the need for stringent cybersecurity policies, advanced protection tools, and continuous professional training. It emphasized the importance of raising awareness and providing specialized training programs to enhance understanding of cybersecurity and effective protection measures, thereby improving overall cybersecurity and safeguarding accounting data.

**Keywords:** Cybersecurity, Accounting Data, Public Accounting, Cyberattacks, Cybersecurity.

**Renforcement de la cybersécurité des données de la comptabilité publique en Algérie : Une analyse comparative des lacunes et des défis avec les pays développés**

**Résumé :** L'étude a révélé que les données comptables sont exposées à de nombreuses menaces, notamment les virus, les attaques par ransomware et la fraude cybernétique, ce qui compromet l'exactitude et la fiabilité des données. Comparée aux pays développés tels que les États-Unis et l'Allemagne, l'Algérie accuse un retard en matière de cybersécurité en raison d'une infrastructure technique insuffisante, d'un manque de personnel spécialisé et de législations et politiques de sécurité faibles. En utilisant une approche analytique comparative, l'étude a évalué les niveaux de cybersécurité en Algérie par rapport aux pays développés, en identifiant les lacunes et les défis clés. Les résultats ont souligné la nécessité de politiques de cybersécurité rigoureuses, d'outils de protection avancés et de formations continues pour les professionnels. Elle a mis en avant l'importance de sensibiliser les travailleurs et de leur fournir des programmes de formation

spécialisés pour améliorer leur compréhension de la cybersécurité et des mesures de protection efficaces, contribuant ainsi à améliorer le niveau de cybersécurité et à protéger les données comptables.

**Mots-clés** : Cybersécurité, données comptables, comptabilité publique, cyberattaques, cybersécurité.

## Introduction:

Cybersecurity is a comprehensive set of measures and technologies designed to protect sensitive data and information from various electronic threats (Craigen, Diakun-Thibault, and Purse, 2014). The importance of this issue has increased due to rapid technological advances and the use of sensitive data in both the public and private sectors (Asaad and Saeed, 2022). Therefore, it is therefore for the government, institutions, and individuals to work diligently to enhance cybersecurity and develop intelligent strategies that address vulnerabilities and ensure the integrity of public accounting data (Demirkan, Demirkan, and McKee, 2020). This requires ongoing awareness and training for all teams working in the field, as well as the adoption of best practices and the use of modern cybersecurity technologies. Strong and comprehensive protection of accounting data is an essential and shared responsibility (Mahieu, Van Hoboken, and Asghari, 2019).

This study is an important tool for improving cybersecurity in Algeria, as it identifies current weaknesses by comparing policies and practices with those of developed countries, helping to identify immediate areas for improvement. The study highlights global protection techniques and strategies, enabling Algeria to adopt best practices for protecting sensitive data. It provides practical recommendations, including encryption, training, firewalls, access control and risk assessment, that will comprehensively improve cybersecurity. In addition, the study will raise awareness of the importance of cybersecurity among decision-makers and employees, reducing the likelihood of breaches and improving the response to threats. It will also help Algeria comply with national and international data protection laws, thereby increasing trust among international partners and citizens. It will also help improve transparency and accountability within government institutions, ensure the continuity of government operations, prevent fraud and corruption, and maintain the stability and security of the economic and social community.

The research methodology used a descriptive-analytical design to explore the challenges and opportunities of cybersecurity and its impact on the protection of public accounting data in Algeria. Data was collected from various sources, including a review of previous literature on cybersecurity and accounting data, and an analysis of reports and studies on cyberattacks on

government institutions in Algeria. In addition, a comparison was made between security practices in Algeria and those in developed countries such as the United States, Germany, Japan and Australia to identify gaps and areas for improvement.

Algeria's public accounting data faces a range of cybersecurity threats, including viruses, ransomware attacks and cyber fraud. Compared to developed countries, Algeria lags behind in cybersecurity due to inadequate infrastructure, lack of specialised personnel, and weak legislation. To improve cybersecurity, it is essential to develop stringent policies, adopt advanced technologies, and provide ongoing training for staff. Raising awareness and training through specialised programmes and awareness campaigns is crucial for data protection. How can Algeria strengthen its cybersecurity to protect its public accounting data in the face of growing cybersecurity threats?

In the context of this study, several hypotheses were proposed to explore the challenges and opportunities of cybersecurity and protection of public accounting data in Algeria. Firstly, public accounting data are exposed to various cybersecurity threats that affect their accuracy and reliability. Secondly, it has been observed that the level of cybersecurity in Algeria lags behind developed countries. Thirdly, the adoption of advanced protection strategies and tools, as well as the development of rigorous policies, can improve this level. Finally, raising awareness and training of public sector employees on the importance of cybersecurity is a crucial step to effectively strengthen the protection of public accounting data.

## 1. Theoretical and Practical Significance

Cybersecurity encompasses all efforts and actions taken to maintain the integrity of electronic systems and data (Jang-Jaccard and Nepal, 2014). It includes protecting against breaches and cyber-attacks, and ensuring a rapid and effective response to any security incidents that threaten our electronic systems and sensitive data. Due to rapid technological advances and significant developments in communication and information, cybersecurity has become a critical issue for individuals, businesses and institutions. As a result, strategies to prevent and combat cyber threats have become fundamental to achieving stability and security in the digital world. These strategies include monitoring unusual activity, early detection of potential breaches and the development of protection systems, encryption and malware defences. They also include immediate response strategies and systematic handling of security incidents to minimise the negative impact. In addition, focusing on data recovery strategies in the event of a breach is essential to ensure system recovery and secure

operations. Ultimately, cyber security is a fundamental concern in today's world, where cyber threats are on the rise. Therefore, everyone should prioritise understanding its concepts and implementing best practices and measures to ensure the complete protection of our data and digital resources.

Public accounting data is one of the most important resources in the public sector. It is necessary to produce precise financial reports that accurately represent the financial situation of public institutions and organizations and to make important financial decisions. These figures are essential for boosting openness and accountability as well as for spotting and defeating corruption. Since public accounting data contains sensitive and important information about public funds, income, and expenditures, security and preservation of this data must be given top priority by the government and the general public. By protecting this data and preventing any breaches or misuses, the stability and integrity of the public accounting system are guaranteed, and trust and transparency between the public, the government, and stakeholders are encouraged.

One of the main features of public accounting data is its accuracy and a high degree of reliability (Krishnan et al., 2005). This is based on the premise that such data is considered to form the basis for active yet cautious financial and managerial decisions. This information thus greatly provides transparency and public accountability, trusted relationship between the government and the people, and fairness as well as flexibility within the public working environment. Besides, this information must be kept with integrity and security for the continuity of government services and long-term success of public policies. Furthermore, public accounting data is a relevant tool for measuring financial performance and analyzing the efficiency of public expenditure for supporting strategic decisions by government entities toward sustainable development (van Ooijen, Ubaldi, and Welby, 2019). It is, therefore, essential that there be an improvement in the quality and security of public accounting data considering increased global challenges in finance to improve transparency for the building of a strong financial system which will result in integrity and credibility in the running of governmental operations.

Algeria faces serious and complex security threats to public accounting data, given that the accounting system is greatly vulnerable to several types of attacks the cyber-attacks direct towards it, hence affecting the reliability and integrity of data (Seffari, 2022). Some of these threats include sophisticated cyber-attacks, accounting data sequences attacks, leakage of vital information, sophisticated malware, and electronic espionage. Considering the nature of these threats, information obtained from public accounting could be at risk of being

lost or even used against the law (St. Pierre and Anderson, 1984); hence, distorting the accuracy of data in communication and posing a threat to the credibility and financial transparency of Algeria. To this regard, the nation of Algeria needs to adopt comprehensive security measures by administering the greatest levels of cybersecurity and technology, developing robust policies, and procedures that can safeguard this sensitive data from potential cyber attacks. Moreover, the importance of good security practices is also imperative for employees and accounting professionals; they need awareness about the importance of data protection, coupled with training for capacity building in this regard. It means cybersecurity of public accounting data to enhance the confidence level in the financial and economic system of Algeria, with a view to ensuring the sustainability of economic and social development within the country.

The types of cyber threats facing public accounting data in Algeria include system breaches, malicious software, and advanced cyberattacks. These threats aim to steal sensitive accounting data or disrupt the public accounting system, negatively impacting the accuracy and comprehensiveness of the financial and accounting information relied upon by government agencies and public institutions for decision-making.

*1.1. Malicious Software and Cyber Threats*

Public accounting data faces various threats from malicious software, including viruses, worms, Trojans, and ransomware. Each type of software represents a unique threat that impacts the accounting system in different ways.

**Viruses** are programs infecting files and replicating when the infected files are executed, thus causing severe system problems. For example, the Melissa virus propagated via infected Microsoft Word documents. When this document was opened, the virus mailed itself to the first 50 people in the victim's email address book, creating a jam in the e-mail systems of big companies and destroying important accounting files, resulting in the loss of financial data and costing huge recovery prices.

**Worms** are self-replicate and don't require user execution; they travel through the networks. One famous case is the WannaCry worm (2017), which exploited a weakness in Windows called "EternalBlue," allowing it to propagate through connected networks and encrypt files. This worm spread to over 230,000 computers in 150 countries, which included hospitals and firms, slowing down government networks and knocking them out, delaying financial reporting.

**Trojans** are programs that, from the user's perspective, appear to be legitimate; however, they contain malware that is now in the complete control of

the attacker. One example is that of the Zeus Trojan, dated back to 2007. It can be used to steal banking data by logging keystrokes. According to reports, this malware led to the theft of millions of dollars from individuals and companies' bank accounts, thus leaking sensitive accounting data or using it in fraud.

**Ransomware** is a certain type of software developed to encrypt data and then demand some money for the key needed for decryption. For example, the so-called Ransomware Petya just encrypts the data and requests a ransom in Bitcoin to have this data decrypted. This particular variant of ransomware managed to attack big organizations like sea ports and oil companies. If the accounting data is encrypted and a ransom requested to decrypt it, this is able to paralyze financial activity and cost an organization millions in losses.

*1.2. Targeted Attacks*

APTs are sophisticated attacks that aim at an organization in order to collect sensitive information over a certain period of time (Chen, Desmet, and Huygens, 2014). For example, in 2014, North Korea conducted a cyber attack against Sony Pictures, from where sensitive data containing unreleased movies and personal e-mails of employees and other stake holders was massively leaked out (Can, 2016). Similarly, APTs can target the financial data of governments and take it for extended periods, risking the financial information and policies of that country.

**Spear phishing** means accordingly that individuals or corporates are tricked into revealing their sensitive information by using well-thought-out emails (Merritt, 2011). For instance, the 2016 attack on the Democratic National Committee—it led to an email scam to get DNC employees' login credentials. This can, in turn, lead to stealing sensitive emails and financial data, and financial fraud can occur.

**Hacking** involves various methods of accessing a system without authorization. Brute Force Attacks are repetitive guesses of passwords, carried out by automated tools against, for instance, SSH accounts, whereby an attacker may gain access to your web servers, thus getting full control that can be used to hack financial systems (Beale and Berris, 2017). Exploits utilize flaws in software or systems to obtain unauthorized access, such as the 2014 Heartbleed attack that exposed sensitive data like private keys and passwords, hence affecting financial systems. SQL injection attacks, like what hit Yahoo! back in 2014, are attacks on database vulnerabilities to scoop up user information that might compromise financial records and systems.

**Network Attacks** include DoS-type network attacks, which bring down systems with an enormous volume of requests (Obaid and Abeed, 2020). For

example, the 2014 attack on Cloudflare disrupted accounting systems, thereby delaying financial data processing. Distributed Denial of Service The 2016 Dyn attack is one such example where a network of Bridges compromised devices was used to flood servers, resulting in requests that disrupt online accounting services and financial operations (Mahjabin et al., 2017). Man-in-the-middle attacks, therefore, are an interception of communications between parties similar to insecure Wi-Fi networks, whose results include the potential theft of financial data or its alteration.

**Identity Attacks** involve the theft of personal identity information and its subsequent misuse (Cassim, 2015). For instance, the 2017 Equifax breach was a clear case of the stealing of personal data for millions of people, and the theft was primarily linked to identity theft with financial fraud involved (Kenny, 2018). Phishing attacks, such as the 2017 Google Docs phishing campaign, are message-deceiving attacks designed for extracting login credentials that might be utilized in stealing financial data or even manipulation.

**Spyware** is software used to secretly track the user's information. For example, Pegasus attacks mobile phones by opening access to cameras, microphones, and messages (Valatsos, 2024). Therefore, this spyware may gather sensitive financial information, hence data leakage and financial fraud.

**Insider threats** come from current or former employees who have the insider information (Shaw, Ruby, and Post, 1998). One example is Edward Snowden, who caused a serious leak of NSA documents back in 2013 (Kont et al., 2015). Typical threats include accessing sensitive financial data for the purpose of committing fraud or other types of information leaks.

**Mobile attacks** involve targeting smartphones and tablets with malware or fake apps (Ahvanooey et al., 2020). A more recent form of malware, the 2016 Triada malware for Android devices, is capable of stealing data and controlling devices remotely (Massarelli et al., 2020). This therefore poses a risk to financial data stored on mobile devices.

**IoT Attacks:** These target vulnerabilities in internet-connected devices, like cameras and smart home controls (Sivaraman et al., 2018). The 2016 Mirai Botnet attack heralded a new frontier in utilizing IoT devices as DDoS bots to collapse huge online services, and holding the potential for the same effect against financial operations and data.

**Social Engineering** is manipulation aimed at human trust to reveal sensitive information or conduct harmful acts (Salahdine and Kaabouch, 2019). The "Business Email Compromise" attack, particularly, involves impersonation of company executives over emails for requests of money transfers or sensitive

information (Al-Musib et al., 2023). This might lead to a financial loss by tricking the financial staff to reveal information or even process fraudulent transactions.

## 2. Analyse data

This research be through the descriptive-analytical research methodology for the study of the challenges and opportunities existing in the domain of cybersecurity and their impacts on the protection of public accounting data in Algeria. Data were collected from different sources: first, through a literature review related to the theme of cybersecurity and accounting data, and secondly, examination of reports and studies published on cyberattacks against the government institutions of Algeria. It has also included cross-country comparison of security practices in Algeria with those adapted in countries like the United States, Germany, Japan, and Australia to identify gaps and points that must be improved.

**Table 1. Comparison of Encryption Techniques and Applications in Different Countries**

| Country | In-transit encryption technologies | Encryption techniques during storage | Examples of encryption applications |
|---|---|---|---|
| United States | 95% strong use of HTTPS and TLS protocols | Use AES and RSA encryption for sensitive information 90% | Government uses strong protocols to protect data during transportation and storage |
| Germany | Use of TLS and VPN protocols 90% | AES encryption for sensitive data 85% | Financial institutions use encryption extensively to protect data |
| Japan | Wide use of HTTPS and TLS 90% | Encrypting data with advanced technologies such as RSA 80% | Data in the public and private sectors is strictly encrypted |
| Australia | Use of TLS/SSL for data transfer 85% | AES and RSA encryption for stored data 80% | Data encryption in critical and government infrastructure |
| Algeria | Increased use of HTTPS and VPN 25% | Limited AES encryption 30% | Limited applications of encryption technologies in government organizations |

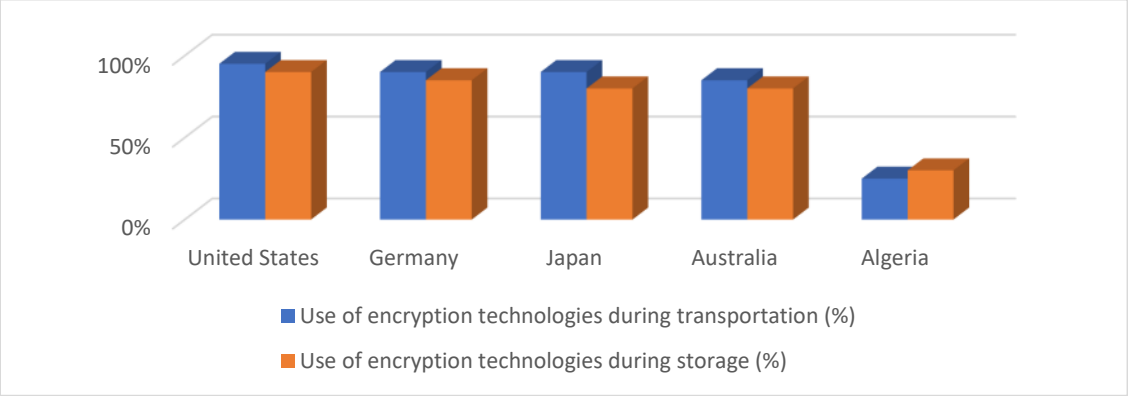


**Figure1.** Using encryption technologies

The figure means that, compared to other countries in the world, Algeria is far behind in the use of encryption technologies. The need for Algeria to increase the use of encryption technologies during transmission and at rest in the government institutions to meet international standards. This can be specifically done by popularizing protocols such as TLS and VPN and also by increasing the usage of AES and RSA technologies.

**Table.2** Comparative Analysis of Employee Training Programs and Cybersecurity Awareness Across Countries

| Country | Annual employee training programs | Cybersecurity awareness among employees | Examples of initiatives |
|---|---|---|---|
| United States | Continuous and extensive training programs 95% | High 90% | Initiatives such as Cybersecurity Awareness Month |
| Germany | Annual intensive training programs 90% | High 85% | Government awareness campaigns and training programs |
| Japan | Periodic Training Courses 85% | Medium to High 80% | Ongoing public and private sector awareness programs |
| Australia | Annual and monthly training programs 90% | High 85% | National awareness programs to address cyber threats |
| Algeria | Limited training programs 30% | Low to Medium 35% | Examples of initiatives |

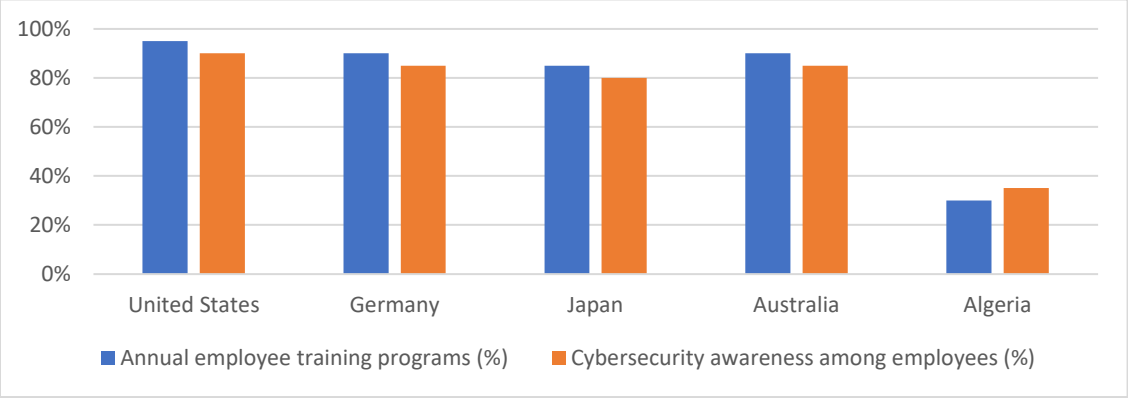


**Figure 2.** Staff training

Algeria is to increase its potentials in training its employees and upgrading the level of awareness regarding the problem, which incomparably stands way below the standard of advanced countries. It could borrow good examples from the United States and Germany in organizing awareness drives and related intensive training programs necessary in improving cybersecurity standards.

**Table 3.** Use of Firewalls, Antivirus Programs, and Security Updates Across Different Countries

| Country | Use of firewalls | Antivirus programs | Security updates |
|---|---|---|---|
| United States | Common and widely adopted 95% | Advanced and multi-application 90% | Daily and Frequent Updates |
| Germany | Extensive use 90% | Advanced programs like Kaspersky and Avira 85% | Frequent updates |
| Japan | Extensive use of firewalls 85% | Advanced applications and continuous monitoring | Frequent updates |
| Australia | Common and widespread use 90% | Advanced apps like Norton and McAfee 85% | Constant updates |
| Algeria | Limited to moderate use 30% | Relatively limited programs 25% | Frequent updates |

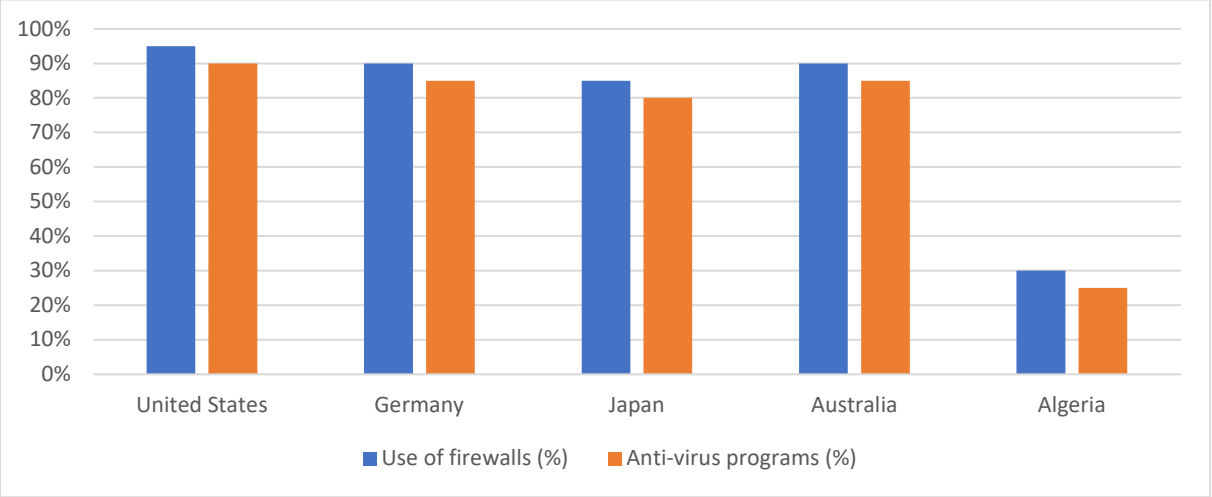


**Figure 3.** Use firewalls and antivirus

The figure shows that, relative to other countries, Algeria has a very minimal usage of firewall and antivirus software. Algeria should increase the usage of advanced firewalls and antivirus programs, ensuring they are updated frequently. Looking at models applied to advanced countries can help in the adoption and implementation of best practices.

**Table. 4** Comparison of Access Control Policies, Applications, and Tools Across Countries

| Country | Access Control Policies | Control applications and tools | Examples |
|---|---|---|---|
| United States | Strict policies 95% | Utilization of IAM and MFA tools 90% | Extensive use of Okta and Azure AD |
| Germany | Strict policies 90% | Use of IAM and MFA technologies 85% | Applications such as PING Identity and RSA |
| Japan | Advanced policies 85% | Using IAM and MFA 80% | Advanced enterprise control technologies |
| Australia | Strict policies 90% | Using IAM and MFA 85% | Tools such as Duo and Google Authenticator |
| Algeria | Limited to moderate policies 30% | Limited technologies 25% | Efforts to optimize access control policies |

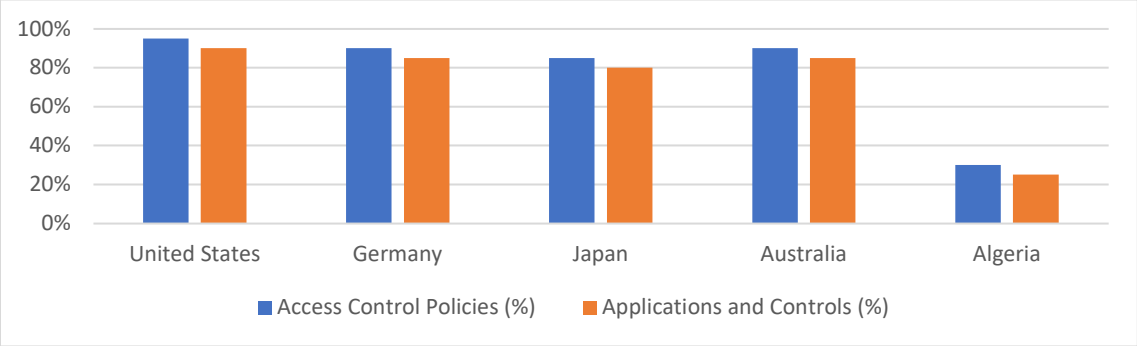


**Figure 4.** Access Control

Data shows that Algeria should enhance access control policies through stringent policies and advanced tools like identity management and multi-factor authentication. This means that the country must work on its access control policies and try to adopt identity management and MFA techniques to protect sensitive data and make it accessible only to authorized personnel.

**Table 5.** Comparison of Frequency and Practices in Periodic Risk Assessments Across Countries

| Country | Frequency of periodic risk assessments | Frequency of periodic risk assessments | Examples |
|---|---|---|---|
| United States | Annual and semi-annual 90% | Annual and semi-annual 90% | Periodic and ongoing risk assessments |
| Germany | Annual 85% | Annual 85% | Continuous assessments and periodic follow-up |
| Japan | Annual 80% | Annual 80% | Using advanced risk assessment tools |
| Australia | Annual and semi-annual 85% | Annual and semi-annual 85% | Continuous and comprehensive risk assessments |
| Algeria | Limited to annual assessments 35% | Limited to annual assessments 35% | Efforts to increase the frequency of risk assessments |

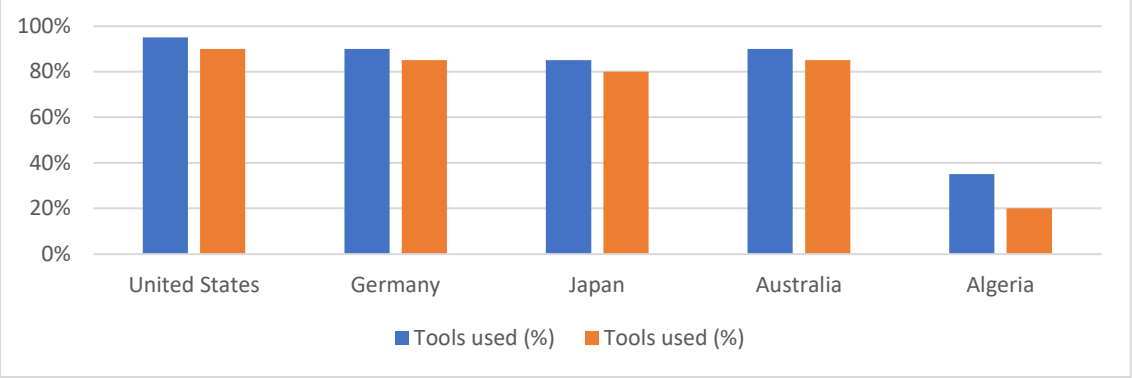


**Figure 5.** Conduct periodic risk assessments

Algeria needs to increase the frequency of risk assessment and begin to involve advanced tools of marker identifier tools in finding security vulnerabilities. Advanced models from nations that implement continuous and comprehensive periodic assessments can be brought into the country to enhance cybersecurity.

**Table 6**. Comparison of the Importance of Financial and Operational Aspects Across Countries

| Importance | Algeria | United States | Germany | Japan | Australia |
|---|---|---|---|---|---|
| Protecting sensitive financial data | Average 40% | High 95% | High 90% | High 85% | High 90% |
| Preventing fraud and corruption | Average 40% | High 95% | High 90% | High 85% | High 90% |
| Ensuring compliance with laws and regulations | Average 40% | High 95% | High 90% | High 85% | High 90% |
| Guaranteeing the continuity of government operations | Average 40% | High 95% | High 90% | High 85% | High 90% |
| Maintaining public trust | Average 40% | High 95% | High 90% | High 85% | High 90% |
| Enhancing transparency and accountability | Average 40% | High 95% | High 90% | High 85% | High 90% |

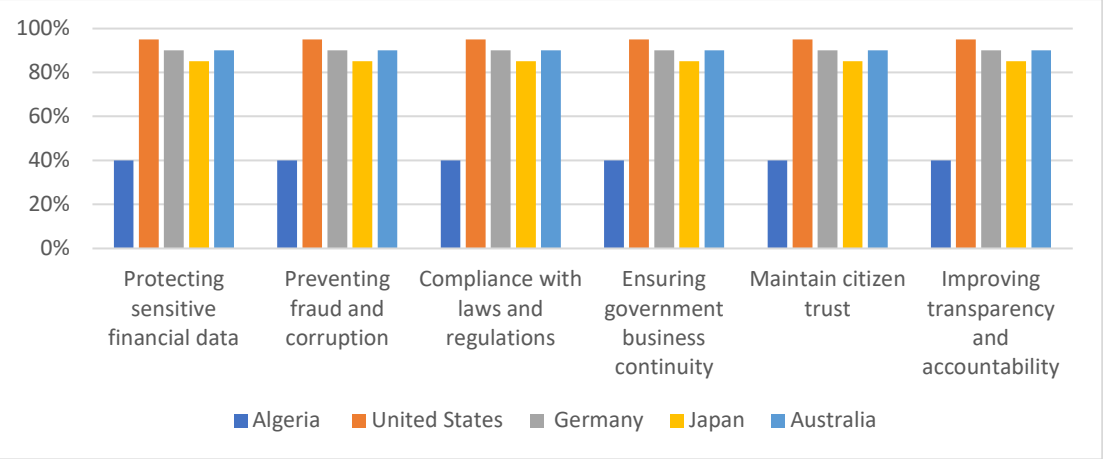


**Figure 6.** The importance of protecting sensitive financial and administrative data

Clearly, Algeria needs to do much more in the protection of sensitive financial and administrative data against irretrievable loss in order to guarantee continuity of government operations, prevent fraud and corruption, comply with laws, and retain citizens' trust. In protecting sensitive financial and administrative data, Algeria should lend more importance to safeguarding data for the prevention of fraud and corruption, ensuring compliance with the law, and retention of public confidence, as well as enhancing transparency and accountability. This can be achieved through improvement in security

infrastructure, developing strict policies, training of employees on a timely basis, and periodical risk assessments.

**Table 7. Accurate Statistical Comparison Between Algeria and These Countries Regarding Cybersecurity Capabilities and Infrastructure**

| Country | Global Cybersecurity Index (GCI) | Investments in Cybersecurity (million dollars) | Number of incident response teams (CERTs) | Cyber Laws and Legislation | International cooperation | Training and awareness |
|---|---|---|---|---|---|---|
| United States | 0.926 | 13000 | 50 | strong | High | Large-scale |
| Germany | 0.908 | 5500 | 30 | strong | High | Medium to High |
| Japan | 0.893 | 4800 | 25 | strong | Medium to High | Medium to High |
| Australia | 0.881 | 2500 | 15 | Strong | Medium to High | Large-scale |
| Algeria | 0.281 | 200 | 2 | Limited | Limited | Limited |

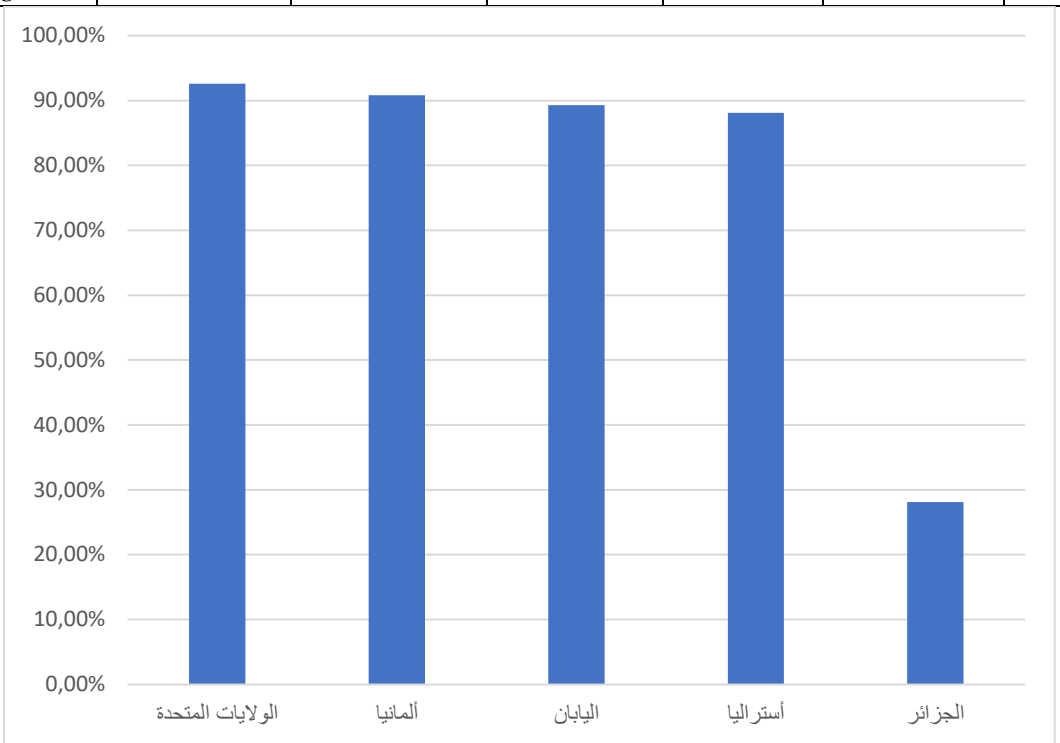


**Figure 7.** Global Cybersecurity Index (GCI)

It means reliance on dependable data originating from a number of sources. I will try to include an estimated table, based on publicly available information, with regard to the cybersecurity capabilities and infrastructure of

each country. Such tables may reflect reports like that by the International Telecommunication Union about the Global Cybersecurity Index, among others by specialized organizations.

**Global Cybersecurity Index GCI**

The leading places in the GCI are held by the USA, Germany, Japan, Australia, etc.; that simply refers to the strength of the cybersecurity infrastructure in those countries. On the other side, Algeria appears at a lower rank, reflecting the need for more in-depth development in that area.

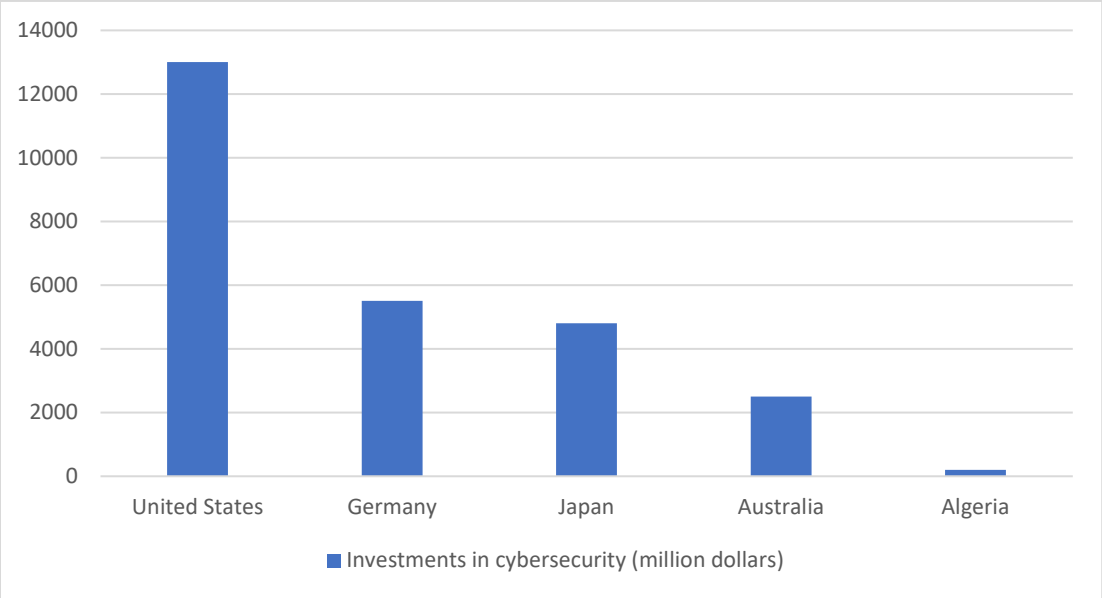


**Figure 8.** Investments in cybersecurity (million dollars)

**Investments in Cybersecurity**

The United States has huge investments in cybersecurity, which helps enhance its defensive capabilities. In comparison, the investments that Algeria makes are meager, hence affecting the country's efforts in trying to curb cybersecurity threats.

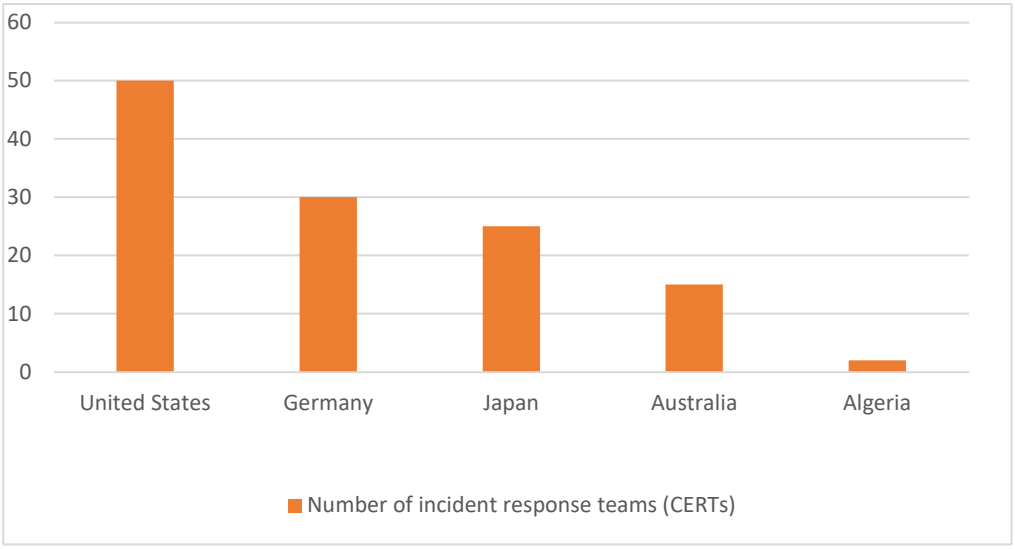


**Figure 9.** Number of incident response teams (CERTs)

**CERTs (Incident Response Teams)**

Advanced countries have multiple CERT teams covering all critical sectors, whereas Algeria has a limited number of CERT teams, hence affecting the speed and efficiency of its response to such attacks. On cybersecurity laws and regulations, advanced countries have strong legal frameworks governing cybersecurity, while Algeria is yet to enhance its legislation in order to improve its legal infrastructure in that direction. At the international cooperation level, advanced countries have high international collaboration in matters of cybersecurity, while Algeria has limited cooperation. This demands strengthened international relationships in order to improve cybersecurity capabilities. Finally, advanced countries have massive investments in training and raising awareness about cybersecurity, while Algeria's training and awareness programs are limited, hence affecting its readiness to tackle cyber threats.

## 3. Discussion

Algeria needs a comprehensive improvement in cybersecurity aspects to enhance its ability to protect government systems and ensure operational continuity effectively. First, an increase in the implemented advanced encryption technologies, such as HTTPS and TLS protocols, at every possible instance for securing the data while it is in transmission is required. This should be supplemented by encrypting sensitive data using more advanced techniques like AES and RSA. It further needs to focus on advanced firewalls and antivirus

software, like Cisco ASA and Palo Alto for the prevention of unauthorized access, and Norton, McAfee, and Kaspersky for malware detection and removal.

Secondly, strict access control policies should be developed by implementing IAM tools and multi-factor authentication, which determine who has access to sensitive financial information. This goes in line with enhancing the issue of training and awareness; it simply means that employees have to be trained in recognizing cyber threats whereby best security practices have to be followed and they organize continuous awareness programs so that people are always cybersecurity aware.

Software should also be maintained up to date at all times to close out any security gaps which may provide entry into the financial systems. Periodic risk assessments should be performed using tools like Nessus and Qualys in order to find security vulnerabilities and take relevant measures on the same.

These can be attained by Algeria by adhering to best practices by advanced countries through more investments in cybersecurity infrastructures and international cooperation. This will involve the development of more effective and pertinent laws and policies related to cyber security in a bid to keep up with the fast-changing technologies.

The relevant structures in Algeria need strengthening of coordination and cooperation, along with further deepening of information and experience exchanges related to fighting cyber threats. In parallel, international cooperation and alliances have to be expanded for knowledge and experience sharing to develop global frameworks of combating cybercrime. Finally, infrastructure development on cyber security, together with specialized expert teams and strategies concerning cyber incident management, is ultimately indispensable toward enhancing cyber security in Algeria. Better resources, backed by augmented funding, could efficiently deal with already existing and evolving cyber threats to rank Algeria among the very top leading nations in the world on cyber security and prepared to face challenges brought forth by the digital age.

**Conclusion**

As cyber threats continue to increase, it is essential for Algeria to adopt advanced strategies and techniques to protect its government systems. Looking at the present scenario in Algeria, in comparison to advanced countries like the United States, Germany, Japan, or Australia, there is a need to build up the security capabilities and follow the best practices in the said area.

The implementation of the proposed recommendations is therefore quite necessary if Algeria is to improve its level of security in cyberspace, ensure compliance with domestic and international laws and regulations, and

strengthen trust among citizens and international partners toward its government institutions. A more transparent and accountable relationship will enhance this bond of trust between citizens and the government, thereby ensuring economic and social stability and security.

In other words, Algeria needs to be in a position to adopt effective measures to consolidate cybersecurity and protect public accounting data. This will involve the government engaging in the institution of effective policies and regulations countering cyber threats, raising awareness, training personnel in this field, and ensuring the institution of best practices in encryption and prevention techniques. Thirdly, Algeria needs to establish international cooperation on this issue of cybersecurity and seek technical assistance from international organizations. Finally, setting up a cyber security infrastructure and adopting innovative strategies for the future shall ensure the security of public accounting data.

**References**

Ahvanooey, Milad Taleby, Qianmu Li, Mahdi Rabbani, and Ahmed Raza Rajput. 2020. "A survey on smartphones security: software vulnerabilities, malware, and attacks." Review of. *arXiv preprint arXiv:2001.09406*.

Al-Musib, Norah Saud, Faeiz Mohammad Al-Serhani, Mamoona Humayun, and NZ Jhanjhi. 2023. "Business email compromise (BEC) attacks." Review of. *Materials Today: Proceedings* 81:497-503.

Asaad, Renas R, and Vaman Ashqi Saeed. 2022. "A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution." Review of. *Applied computing Journal*:227-44.

Beale, Sara Sun, and Peter Berris. 2017. "Hacking the Internet of Things: Vulnerabilities, dangers, and legal responses." Review of. *Duke L. & Tech. Rev.* 16:161.

Can, Murat. 2016. "The unbearable lightness of cyber: Cyberspace and state sovereignty." Review of.

Cassim, Fawzia. 2015. "Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?" Review of. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad* 18 (2):68-110.

Chen, Ping, Lieven Desmet, and Christophe Huygens. 2014. A study on advanced persistent threats. Paper presented at the Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15.

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. 2014. "Defining cybersecurity." Review of. *Technology innovation management review* 4 (10).

Demirkan, Sebahattin, Irem Demirkan, and Andrew McKee. 2020. "Blockchain technology in the future of business cyber security and accounting." Review of. *Journal of Management Analytics* 7 (2):189-208.

Jang-Jaccard, Julian, and Surya Nepal. 2014. "A survey of emerging threats in cybersecurity." Review of. *Journal of computer and system sciences* 80 (5):973-93.

Kenny, Caitlin. 2018. "The Equifax data breach and the resulting legal recourse." Review of. *Brook. J. Corp. Fin. & Com. L.* 13:215.

Kont, Markus, Mauno Pihelgas, Jesse Wojtkowiak, Lorena Trinberg, and Anna-Maria Osula. 2015. "Insider threat detection study." Review of. *NATO CCD COE, Tallinn*.

Krishnan, Ramayya, James Peters, Rema Padman, and David Kaplan. 2005. "On data reliability assessment in accounting information systems." Review of. *Information Systems Research* 16 (3):307-26.

Mahieu, Rene, Joris Van Hoboken, and Hadi Asghari. 2019. "Responsibility for Data Protection in a Networked World: On the Question of the Controller, Effective and Complete Protection and Its Application to Data Access Rights in Europe." Review of. *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 10:84.

Mahjabin, Tasnuva, Yang Xiao, Guang Sun, and Wangdong Jiang. 2017. "A survey of distributed denial-of-service attack, prevention, and mitigation techniques." Review of. *International Journal of Distributed Sensor Networks* 13 (12):1550147717741463.

Massarelli, Luca, Leonardo Aniello, Claudio Ciccotelli, Leonardo Querzoni, Daniele Ucci, and Roberto Baldoni. 2020. "Androdfa: android malware classification based on resource consumption." Review of. *Information* 11 (6):326.

Merritt, David T. 2011. "Spear phishing attack detection." Review of.

Obaid, Hadeel S, and Esamaddin H Abeed. 2020. "DoS and DDoS attacks at OSI layers." Review of. *International Journal of Multidisciplinary Research and Publications* 2 (8):1-9.

Salahdine, Fatima, and Naima Kaabouch. 2019. "Social engineering attacks: A survey." Review of. *Future internet* 11 (4):89.

Seffari, Asma 2022. "Information Security and the need to move towards the application of Standard Specifications in Algerian institutions." Review of. *Humanities Journal of the University of Oum El Bouaghi* 9 (2):18-34.

Shaw, Eric D, Keven G Ruby, and Jerrold M Post. 1998. "The insider threat to information systems." Review of. *Security Awareness Bulletin* 2 (98):1-10.

Sivaraman, Vijay, Hassan Habibi Gharakheili, Clinton Fernandes, Narelle Clark, and Tanya Karliychuk. 2018. "Smart IoT devices in the home: Security and privacy implications." Review of. *IEEE Technology and Society Magazine* 37 (2):71-9.

St. Pierre, Kent, and James A Anderson. 1984. "An analysis of the factors associated with lawsuits against public accountants." Review of. *Accounting Review*:242-63.

Valatsos, Vasileios. 2024. "Spyware technologies." Πανεπιστήμιο Πειραιώς.

van Ooijen, Charlotte, Barbara Ubaldi, and Benjamin Welby. 2019. "A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance." Review of.