Economics and Management
ISSN:2683-1325
Volume: XXI, Issue:2, Year:2024, pp.87-105
DOI: 10.37708/em.swu.v21i2.6

INVESTIGATING YOUNG ENTREPRENEUR'S AWARENESS OF CYBERSECURITY: A FOCUS ON STUDENT START-UP PROJECTS

Belgoum Farid[1], Adnani Nizar Djalal[2], Benessalah Nawel[3]

Received: 21.07.2024, Accepted: 01.11.2024

Abstract

This study investigates the level of cybersecurity awareness among young Algerian entrepreneurs who founded start-ups within university ecosystems. These entrepreneurs are typically assumed to have a higher knowledge base in this domain due to their academic background. We examine five key factors influencing cybersecurity: importance, knowledge, resources, culture, and impact on start-ups. A questionnaire was distributed to 51 young entrepreneurs across various sectors. Statistical techniques were employed to analyze the results. The findings show that while student entrepreneurs have some cybersecurity awareness, there is a considerable knowledge and resource gap. This vulnerability exposes their projects to an increased risk of cyber-attack. Based on the findings, the study suggests a collaborative strategy. Universities and socioeconomic partners should share responsibilities for improving entrepreneurs' cybersecurity skills. This united endeavour will create a safer environment for start-up development while contributing to worldwide growth.

Keywords: *Cybersecurity; Start-up; Awareness; Entrepreneurs; Projects; University.*
JEL Codes: M13 ; L26 ; O31.

Introduction

Cybersecurity is linked to the dimensions of the economy, especially the shift to the knowledge economy, which has adopted information and communication technologies as a means of developing the organization through processed and stored data for use according to specific strategies related to increasing production, controlling costs, gaining customer satisfaction, securing used machines and means of payment, and other

[1] Prof, Research laboratory applied to the Firm, the Industry and the Territory, University of Oran 2 - Algeria, farid.belgoum@univ-oran2.dz, ORCID ID: 0000-0002-8918-2255
[2] Lecturer, University of Oran 2 - Algeria, adnani.djalal@univ-oran2.dz, ORCID ID: 0009-0002-8108-4703
[3] Lecturer, Research laboratory applied to the Firm, the Industry and the Territory, University of Oran 2 - Algeria, benssalah.nawel@univ-oran2.dz,ORCID ID: 0000-0002-4886-4970

goals that can be achieved. It is disrupted due to the risk of electronic attacks. Thus, the importance of cyber security arises which accompanies the organization's activity in all of its stages to secure various operations.

Moreover, the rise in cybersecurity incidents has significantly boosted top executives' engagement and increased the awareness of cybersecurity challenges on a large scale. With time, cybersecurity has evolved from a problem at the operational level to a constant strategic concern, involving influential internal (executives, for example) and external (stakeholders) agencies (Zhang, 2020). When awareness of the significance of cybersecurity results in new laws, inclusion in curriculum, training courses, and promotional materials for mobile banking and telecommunications companies, the program is considered sustainable (Changa & Coppel, 2020). For this, it is advised to raise Internet security awareness by teaching users about the many cyber threats and vulnerabilities of computers and data, given society's growth and the changing nature of digital culture (Zhang-Kennedy & Chiasson, 2020).

In this context, recent studies showed a lack of awareness of cybersecurity among university students (Binti Sirat, Othman, Dauda, & Garba, 2020; Mendoza, Roque Hernández, Quezada, & Salazar Hernández, 2023; Hnaif, Derbas, & Almanasra, 2023; Shun Xiang & Hasbullah, 2023), Others highlighted the importance of technical aspects, which exclude the consideration of human factors in cybersecurity. (Jeong, Mihelcic, Oliver, & Rudolph, 2019; Pollini et al., 2022)

However, this paper focuses on students specifically involved in start-up projects. These students might have a higher level of cybersecurity awareness due to the inclusion of workshops on platform/website creation within their university incubator training program.

This paper aims to:

- Provide an overview of cybersecurity ideas applicable to organizations. This clarifies the focus on business concepts.
- Create a preliminary framework for evaluating cybersecurity awareness among start-ups formed by young entrepreneurs and suggest methods to enhance it.

Literature review

Cybersecurity awareness

Cybersecurity is a science searching how to protect information provided and used by companies and keep systems safe from threats. Therefore, there are more investments in this field worldwide through means, tools, and procedures to ensure the protection of the whole. It has become a strategic element that several organizations give importance to; the increasing growth of automated media technologies in various sectors makes cybersecurity an utmost

necessity because it protects data from theft and damage, including sensitive personal data, financial and intellectual property, and internal information systems.

Menasri (2023) research highlights that cybersecurity was not a significant concern in the early days of computing due to a lack of information about hacking threats. However, the advent of hacker culture in the 1980s and 1990s, driven by research and curiosity, revealed system weaknesses. As technology advanced in the 2000s, digitalization increased the demand for comprehensive cybersecurity. The risk of sensitive data being kept and transmitted online became more apparent. High-profile cyber-attacks in the late 2000s and early 2010s demonstrated the terrible implications of breaches, resulting in a global growth in cybersecurity awareness.

According to Algerian legislation, cybersecurity includes tools, policies, security concepts, security mechanisms, guidelines, risk and business management methods, training, good practices, safeguards and technologies that can be used to protect electronic communications against any event that would compromise the availability, integrity and confidentiality of the processing or transmission (Law No. 18-04, 2018).

The Global Cybersecurity Index (GCI), first released in 2015, identifies cybersecurity growth areas and best practices to strengthen nations' commitment to cybersecurity. The five pillars listed below serve as the main areas of national cybersecurity pledges according to the Global Cybersecurity Index:

Figure no.1 The five pillars of cybersecurity

Source: ITU-D. (2023). Cybersecurity Program Global Cybersecurity Index – GCIv5 Reference Model (Methodology). Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2E.pdf

Legal measures: legislative instruments, including law, rules and policies.

Technical measures: Technical institutions and frameworks can be used to measure technical measures.

Organizational measures: the existence of institutions and strategies coordinating cybersecurity development at the national level can be utilized to evaluate the effectiveness of the organizational measures.

Capacity development: includes the advancement of knowledge and abilities among the general public, individuals, professionals whose job involves cybersecurity professionals (ITU-, 2023).

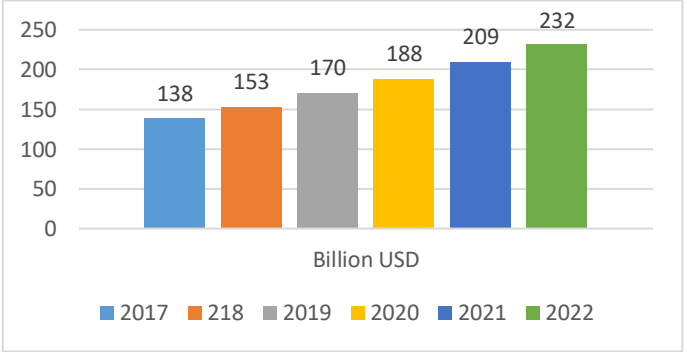
Cooperation measures: enhance dialogue and coordination, enabling the creation of a more comprehensive cybersecurity field of application.

Generally, cybersecurity aims to secure cyberspace, including digital services, by protecting data and systems' confidentiality, integrity, and availability. This encompasses maintaining user privacy, ensuring the legitimacy of electronic actions, and fostering trust in online applications and transactions. Additionally, cybersecurity aims to establish robust security policies and procedures for organizations and countries, ultimately promoting economic growth (Boudaoud, Dahou, & Souag, 2021).

The cybersecurity market is constantly growing, and new trends are emerging yearly. Additionally, being one of the industries' most rapidly expanding markets, it is predicted to expand with developing and established nations' rising internet adoption rates. While writing off cybersecurity as an IT department responsibility was customary, it is progressively taking centre stage in top-level strategic planning. As corporations and governments scramble to secure their networks, a booming market has opened for cybersecurity solutions (Bailetti & Zijdemans, 2014).

Figure no. 2 depicts a significant upward trend in the global cybersecurity market. From 2017 to 2022, the market value nearly doubled, increasing from USD 138 billion to USD 232 billion. This rapid growth highlights the growing importance of cybersecurity solutions in today's digital landscape.

Figure no. 2 Size of the cybersecurity market worldwide from 2017 to 2022



Source: Moiseienko, T., & Kiva, A. (2021). Cybersecurity Startup Investments. Cybersecurity Providing in Information and Telecommunication Systems, in Size of the cybersecurity market worldwide, Statista, 2021.

Table no. 1- GCI results (2020): Global score and rank Africa region (some first contraries) (ITU, 2021)

Rank	Country (Global)	Score	Rank	Country (Africa)	Score
1	United States of America	100	1	Mauritius	96.89
2	United Kingdom	99.54	2	Tanzania	90.58
2	Saudi Arabia	99.54	3	Ghana	86.69
3	Estonia	99.48	4	Nigeria	84.76
4	Korea (Rep. of)	98.52	5	Kenya	81.7
4	Singapore	98.52	6	Benin	80.06
4	Spain	98.52	7	Rwanda	79.95
5	Russian Federation	98.06	8	South Africa	78.46
5	United Arab Emirates	98.06	9	Uganda	69.98
5	Malaysia	98.06	10	Zambia	68.88
6	Lithuania	97.93	11	Côte d'Ivoire	67.82
7	Japan	97.82	12	Botswana	53.06
8	Canada**	97.67	13	Cameroon	45.63
9	France	97.6	14	Chad	40.44
10	India	97.5	15	Burkina Faso	39.98

Source: ITU. (2021). Global Cybersecurity Index 2020. Geneva. Retrieved from https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

The table shows the Global Cybersecurity Index scores for different countries. The United States of America gets the highest global score (100), while 97.5 is the lowest recorded globally. Mauritius has the most incredible score in Africa (96.89), while Burkina Faso has the lowest score (39.98). It demonstrates a huge discrepancy in the cybersecurity preparedness of leading countries and African nations.

Algeria ranked 104 with a score of 33.95, indicating the need to make efforts in this area with the rational transformation to the use of electronic services.

In this context, (Law No. 09-04, 2009) aims to set rules to prevent and combat problems related to information and communication technologies. This including:

- Information system: any separate system or group of interconnected or systems. One or more of them involves automated processing of data to implement a specific program.
- Informational data: Any process of presenting facts, information, or concepts in a form ready for processing within an information system, including computer programs. A proportion that would make an information system perform its function.

- Data related to the movement of the system: any data related to communication through an information system produced by this. The latter is considered a part of a communications cycle, explaining the source of the communication, the destination to which it is sent, the route it takes, the time, date, volume, duration of the communication, and the type of service.

Cybersecurity's challenges awareness:

In information security, awareness refers to the user's ability to recognize or prevent behaviours that jeopardize cyber security. Users' awareness is critical to sensitizing them to associated issues and empowering them to gain adequate knowledge about what related systems are doing and sharing (Liu, Nikitas, & Parkinson, 2020).

Over the past few decades, practitioners and researchers have created a wide range of multimedia teaching tools aimed at non-expert end users to close the knowledge gap in cybersecurity and raise awareness (Zhang-Kennedy & Chiasson, 2020).

Research suggests that successful cybersecurity awareness campaigns hinge on several key factors (Changa & Coppel, 2020):

- Professional Development: Campaigns should be well-planned and organized for maximum impact.
- Focus on Positive Reinforcement: Fear-based tactics are ineffective.
- Engaging Education: More than simply providing information is required. Training should be targeted and actionable, and users should be provided with clear steps. Feedback is also crucial.
- Ongoing Support: Once users are receptive to change, continuing training and feedback are essential to maintain engagement.
- Cultural Sensitivity: Campaigns should be tailored to different cultural contexts and user characteristics.

Sereir El Hirtsi (2023) highlighted some challenges to increase awareness of cybersecurity in Algeria:

- Protecting businesses: Providing cybersecurity resources and protection for small and medium enterprises (SMEs).
- Boosting investment: Encouraging investment in cybersecurity solutions to strengthen national defences.
- Developing a skilled workforce: Investing in education and training to create a pool of qualified cybersecurity professionals.
- Fostering innovation: Establishing business incubators to support cyber-focused companies and opening university programs in cybersecurity.

Cybersecurity start-up

Entrepreneurship has grown significantly as organizations have been compelled to change their strategies to keep competitive and expand beyond the traditional business management model in order to contribute to supporting the economy (Saoud & Meddahi, 2023). In today's digital age, understanding entrepreneurship requires a multifaceted approach (Taylor-Wesselink & Teulon, 2022). The new task has been implementing a business plan to produce new ideas, limit costs, and decrease risks (Orero-Blat, Palacios-Marqués, & Garzón, 2021). This environment of digitalization is creating new ways of exchanging information and altogether new approaches to innovation processes, both within organizations and at the interface with universities or end customers (Schroth & Häußermann, 2018).

As a result of this modern business, start-ups appeared to help countries achieve long-term success. This is due to their potential to create jobs and contribute to national economy.

The start-up landscape is thriving due to mounting economic pressures and the rapid advancement of technology. However, concerns remain regarding the reliability of established and emerging technologies, especially in light of the increasing frequency of cybersecurity breaches. Consequently, start-ups are aggressively investing in the cybersecurity of their new and current digital assets (Nelson & Madnick, 2017; Norval, Janssen, & Singh, 2021).

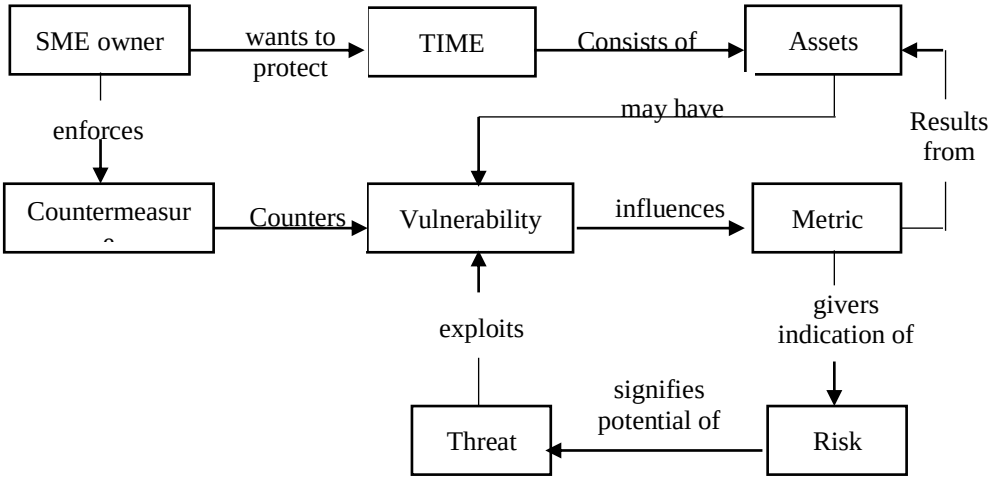
An extensive review of 24 research articles published between 2011 and 2022 found no single framework comprehensively assessing cybersecurity maturity in tech start-ups. While some frameworks share similarities in maturity levels, a gap exists for a unified approach (Marican, Abd Razak, Selamat, & Othman, 2023).

This is why it is essential to consider the security aspects of information security and the compliance dimensions of governance to ensure the application of appropriate policies and procedures with continuous improvement (Jayalath & Premaratne, 2021).

Ozkan & Spruit (2023) discuss start-ups that cannot defend their company against cyber-attacks because they need more financial resources to invest in cyber security. Pratomo (2023) highlights that adequate cybersecurity measures must be put in place by organizations which use digital platforms for financial transactions and information storage. For this reason, instead of focusing their efforts on major corporations, hackers are instead targeting start-ups and other smaller organizations (Marican, Othman, Selamat, & Abd Razak, 2023)**.**

Figure 3 depicts the way the vulnerability-threat-control paradigm helps us assess cybersecurity risk. Assets have weaknesses (vulnerabilities) that attackers (threats) can exploit, causing harm. By measuring these vulnerabilities (cybersecurity metrics), we can understand the risk to an asset. The higher the metric, the greater the risk of a threat exploiting the vulnerability. To address this risk, SME owners can implement controls (countermeasures) to mitigate it.

Figure no. 3 View on cyber-systems to fit a threat-based cybersecurity risk assessment approach for SMEs- Start-ups



Source: Haastrechtet al. (2021). A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. Proceedings of the 16th International Conference on Availability, Reliability and Security, p: 3. doi:https://doi.org/10.1145/3465481.3469199

Education cybersecurity

Given the importance of cyber security, universities, training centres, and even companies are prioritising it in their training programs.

Changa & Coppel (2020) discuss the importance of security education, which must be focused, possible, actionable, and providing feedback. Guo & Tinmaz (2023) showed that teaching cybersecurity in colleges can significantly benefit students. This education equips them with safe online habits and helps them understand the risks of neglecting cybersecurity. The study highlights the need for targeted programs to address students' weaknesses, further enhancing their online safety. More work has to be done to educate

the public, especially students, about cybersecurity and responsible internet usage (Ahamed et al., 2024).

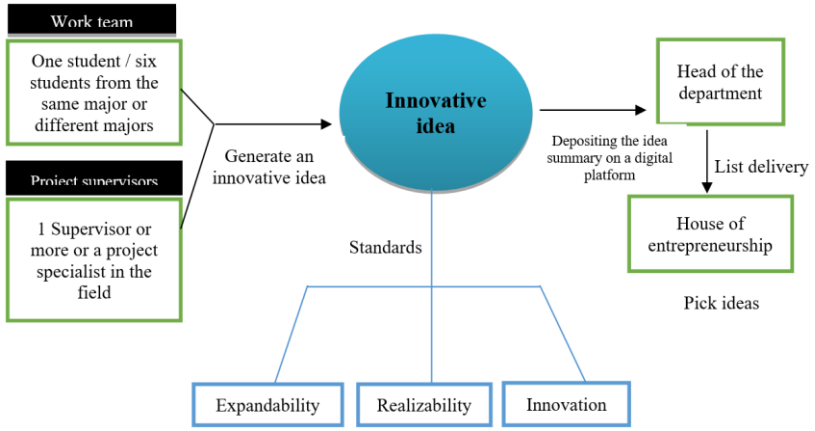
According to a study by Moallem (2019), college students need to be aware of how to protect their data, even if they think that they are watched when they use the Internet and that their data is not safe even on university servers. Furthermore, academic institutions are not actively working to raise college students' awareness of these problems and teach them how to defend themselves against possible cyber-attacks. This approach makes universities responsible even though organizations also create a space for collaboration in training.

Research Methodology

In Algeria, every university has incubators to help with start-up development. The university's incubator intends to boost student innovation by increasing the number of patents registered annually.

A graduation thesis project with a start-up focus combines university degree requirements with entrepreneurship training. This approach aims to cultivate students' entrepreneurial skills and create innovative businesses based on technology and problem-solving (Brachouche, Moussa, & Belgoum, 2024). Students develop a business model, marketing strategy, and financial plan, culminating in a pitch to a jury for funding and potential incubation. Figure 4 shows the process of creating a start-up at an Algerian University.

Figure no. 4 Stages of registering a start-up idea at the university



Source: Belgoum, F., & Benessalah, N. (2023). Start-up and patent degrees' initiative in Algeria: supporting business innovation and creation among university students. Entrepreneurship, 11(1), 21-30. doi:https://doi.org/10.37708/ep.swu.v11i1.2

Sample and data

We chose current graduate (license and master) students known as generation (Z) students, according to Mendoza, Roque Hernández, Quezada, & Salazar Hernández (2023), who are digital natives; they grew up in a technical environment. We distributed 51 questionnaires to a sample of 150 projects registered at the university. Of these projects, 34% were assessed as ready on a managerial and technical level. The distribution by sector and number of employees is shown in the graphs below.

Figure 5. Startup Distribution by Business Sector

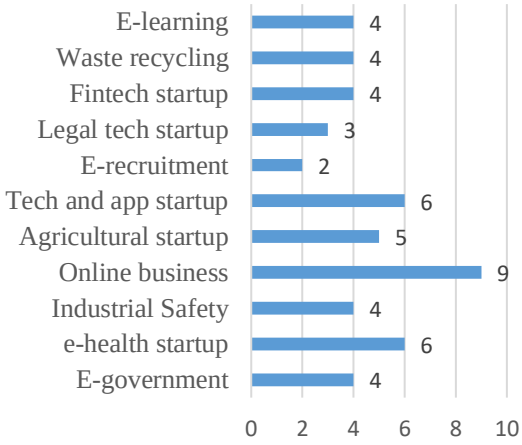
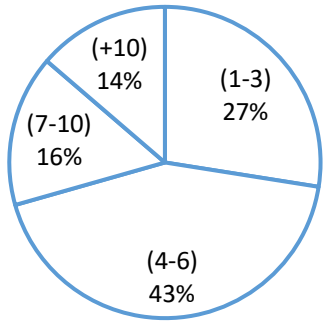


Figure 6. Employee Distribution (%)



Source: compiled by the authors

Measurement

A structured questionnaire will be administered to comprehend the interaction between factors influencing cybersecurity awareness thoroughly. This questionnaire will gather data on several crucial factors: The importance of Cybersecurity, Cybersecurity Knowledge, Cybersecurity Resources, Cybersecurity Culture and the Impact of Cybersecurity.

Each element will be measured using a five-point Likert scale to assess participants' responses. The Likert scale typically runs from "Strongly Disagree" (1) to "Strongly Agree" (5).

Based on their total questionnaire score, start-ups can be classified into various categories of cybersecurity preparedness. Those with low scores are thought to have weak

defences and are highly vulnerable to attacks. Start-ups with high scores are believed to have solid defences and are significantly better protected.

Results and Discussion

Results

To analyze the responses from our sample, we employed a multi-step approach. First, we assessed the reliability of our data using reliability tests. This ensures that the data is consistent and can be trusted. Next, we calculated the means for each variable to estimate the respondents' overall level of cybersecurity awareness.

Following this, we conducted an Analysis of Variance (ANOVA) to identify any statistically significant differences in cybersecurity awareness levels across start-up sectors or study factors. Finally, we calculated correlation coefficients to explore the relationships between various variables and cybersecurity awareness.

Table no. 2 - Reliability Statistics

Factors	Cronbach's Alpha	N of Items
Importance of Cybersecurity	0.779	3
Cybersecurity Knowledge	0.889	3
Cybersecurity Resources	0.879	3
Cybersecurity Culture	0.885	3
Impact of Cybersecurity	0.891	3

Source: compiled by the authors (SPSS25)

The Cronbach's Alpha reliability statistic measures a scale's internal consistency. The table above shows that a number between 0.779 and 0.891 indicates high reliability, which means that the scale's components consistently measure the same underlying concept.

Table no. 3 - Descriptive Statistics

Factors	N	Mean	Std. Deviation
Importance of Cybersecurity	51	3,2745	1,19388
Cybersecurity Knowledge	51	2,5294	1,13759
Cybersecurity Resources	51	2,8889	,96762
Cybersecurity Culture	51	3,7778	1,06805
Impact of Cybersecurity	51	4,0131	1,16802

Source: compiled by the authors (SPSS25)

Analysis of Cybersecurity Knowledge and Resources:

The findings indicate a gap in knowledge regarding cybersecurity among student entrepreneurs. This translates to a lack of necessary information to protect their start-ups, including measures, such as:

- Implementing effective cybersecurity measures.
- Training employees on good cybersecurity practices.
- Identifying and mitigating cyber-attack risks.

The average score (2.88) for resource access suggests that students need more tools and support to implement robust cybersecurity practices. This could include limitations in:

- Affording effective cybersecurity solutions.
- Finding qualified cybersecurity experts for assistance.
- Positive Indicators.

Despite the knowledge and resource gaps, the high score (3.27) for the perceived importance of cybersecurity reflects a positive understanding. Students recognize the need for:

- Prioritizing cybersecurity for their start-ups.
- Implementing relevant security measures.
- Mitigating cyber risks.

The high score (3.77) for cybersecurity culture suggests that students value information security and incident response. This indicates an awareness of:

- The importance of protecting sensitive business information.
- The need to report and address cybersecurity incidents proactively.
- The positive Impact of Cybersecurity.

The satisfactory score (4.01) for the impact of cybersecurity highlights its perceived benefits for start-ups. Students acknowledge the positive influence on:

- Building a solid reputation.
- Gaining customer trust.
- Minimizing financial losses due to cyber-attacks.

Analysis of Variance (ANOVA) was used to compare the means of cybersecurity awareness levels among businesses across five categories: legal tech, online business, waste recycling, fin-tech, and agricultural start-ups.

Table no. 3- Analysis of Variance ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Importance of Cybersecurity	Between Groups	49,851	10	4,985	9,311	,000
	Within Groups	21,417	40	,535		
	Total	71,268	50			
Cybersecurit	Between Groups	43,058	10	4,306	7,956	,000

y Knowledge	Within Groups	21,648	40	,541		
	Total	64,706	50			
Cybersecurity Resources	Between Groups	32,703	10	3,270	9,270	,000
	Within Groups	14,112	40	,353		
	Total	46,815	50			
Cybersecurity Culture	Between Groups	49,248	10	4,925	25,289	,000
	Within Groups	7,790	40	,195		
	Total	57,037	50			
Impact of Cybersecurity	Between Groups	60,825	10	6,082	32,928	,000
	Within Groups	7,389	40	,185		
	Total	68,214	50			

Source: compiled by the authors(SPSS25)

The results revealed a statistically significant difference ($p < 0.05$). A post-hoc analysis using Least Significant Difference (LSD) identified higher levels of cybersecurity awareness in legal tech, online businesses, waste recycling, and fin-tech businesses. Conversely, agricultural start-ups needed to exhibit higher levels of awareness. This may be attributed to a greater focus on product development without prioritizing project security.

Table no. 4 - Correlation

		Importance of Cybersecurity	Cybersecurity Knowledge	Cybersecurity Resources	Cybersecurity Culture
Impact of Cybersecurity	Pearson Correlation	,777**	,351*	,534**	,909**
	Sig. (2-tailed)	,000	,012	,000	,000
	N	51	51	51	51

Source: compiled by the authors(SPSS25)

Note*. Correlation is significant at the 0.05 level (2-tailed).

The correlation analysis indicates a positive relationship between cybersecurity factors and cybersecurity impact. This suggests that businesses with more robust cybersecurity measures experience a more positive impact from those measures. It highlights the importance of prioritizing security within businesses.

However, the analysis also suggests that cybersecurity knowledge and resources can be improved. More efforts are needed to enhance these dimensions and ensure a robust cybersecurity posture.

Discussion

Our study highlights a critical discrepancy between students' awareness of cybersecurity's importance and the knowledge and resources they possess to implement it effectively in their projects. While students demonstrate a positive understanding of the need for a strong cybersecurity culture, they need more practical skills and tools to translate this awareness into action.

To bridge this gap and equip students with the necessary cybersecurity skillset, we recommend incorporating security awareness training directly into their academic programs. Cybersecurity experts should deliver this training through engaging workshops complemented by ongoing support as students develop their projects.

A comprehensive plan is required to build a strong cybersecurity culture, which involves educating individuals about internet threats, providing frequent training on cybersecurity best practices, and encouraging cooperation and open communication (Selvan & Fonceca, 2023). As cybersecurity is a rapidly expanding sector of the employment market, and the cybersecurity skills shortage is a global concern, a new method is required to develop the cybersecurity labour force (Da Veiga et al., 2021).

Nobles (2019) analyzes the role of human knowledge. Failure to appreciate the importance of human factors in the field of cybersecurity threatens the existence of institutions, as cybersecurity operations have expanded and become more ambiguous from a technological standpoint, which leads to an increase in the chances of human errors.

While initiatives like the university's recently introduced platform creation training are commendable, they must comprehensively address the broader cybersecurity challenges start-ups face. A more robust approach is required, encompassing platform security and integrating the latest information security techniques throughout every stage of the business development process.

Conclusion

Modern technology has become more prevalent, resulting in a new virtual world alongside the physical one. This "cyberspace" arose from the digital revolution, resulting in an information flood. The ease of accessing information through several communication platforms is unprecedented (Albada & Eleyan, 2024).

Our study revealed a positive cybersecurity awareness among student start-up projects. Students demonstrated a clear understanding of the importance of cybersecurity and a culture of developing information security practices. However, there is a critical

need to enhance students' cybersecurity knowledge and provide them with technical and human resources.

This gap highlights the importance of initiatives to train and develop the next generation of cybersecurity professionals, as discussed by (Ng & Kwok, 2017; Belgoum, Entrepreneurship Education in Algeria: Between the perspectives of the University and the Accompanying Partners, 2020). Additionally, implementing the ISO/IEC 27001 information security framework, as endorsed by (ISO/IEC, 2022), can strengthen student start-ups' cybersecurity posture. This globally recognized standard promotes proactive risk management, protects critical assets, and ensures data confidentiality, integrity, and availability.

Universities worldwide recognize the value of equipping students with entrepreneurial training to launch their businesses (Shenkoya, Hwang, & Sung, 2023). However, the responsibility for fostering cybersecurity awareness among student entrepreneurs extends beyond universities. A collaborative strategy involving governmental bodies, training centres and private firms is crucial for achieving this goal.

REFERENCES

Ahamed, B., Pola, M. R., Kabir, A. I., Sohel-Uz-Zaman, A. S., Al Fahad, A., Chowdhury, S., & Rani, D. M. (2024). Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era. *Sage Open, 14*(1). DOI: https://doi.org/10.1177/21582440241228920

Albada, O., & Eleyan, D. (2024). Cybersecurity Awareness of Vulnerabilities: Attacks, Solutions and Cybersecurity Behavior in Palestine: *Literature Review*. Retrieved from https://www.researchgate.net/publication/377761598

Bailetti, T., & Zijdemans, E. (2014). Cybersecurity Startups: The Importance of Early and Rapid Globalization. *Technology Innovation Management Review, 4*(11), pp. 14-21. DOI: 10.22215/time review/845

Belgoum, F. (2020). Entrepreneurship Education in Algeria: Between the Perspectives of the University and the Accompanying Partners. *Advanced Research in Economics and Business Strategy Journal,* 01(01), pp. 15-22. DOI: https://doi.org/10.52919/arebus.v1i01.7

Belgoum, F., & Benessalah, N. (2023). Start-up and patent degrees initiative in Algeria: supporting business innovation and creation among university students. *Entrepreneurship,* 11(1), pp. 21-30. DOI:https://doi.org/10.37708/ep.swu.v11i1.2

Binti Sirat, M., Othman, S., Dauda, I., & Garba, A. (2020). Cyber security awareness among university students: a case study. *4th Asia International Multidisciplinary Conference. Science Proceedings Series* 2(1), pp. 82-86. Available at: https://www.researchgate.net/publication/342242874_CYBER_SECURITY_AWARENESS_AMONG_UNIVERSITY_STUDENTS_A_CASE_STUDY

Boudaoud, B., Dahou, S., & Souag, A. (2021). Constructive modeling of the contribution of the cybersecurity dimensions of data to achieving electronic consumer satisfaction by enhancing trust as a mediating variable. *Journal of Business Administration and Economic Studies, 7*(1), 829-852. Retrieved from https://www.asjp.cerist.dz/en/article/154023

Brachouche, B., Maamri, M. & Belgoum, F. (2024). Dynamics and challenges of family businesses in Algeria: A multidisciplinary analysis of the literature (2008-2023). *Economics and management*, 21 (1), pp. 55-75. DOI: 10.37708/em.swu.v21i1.5

Changa, L., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers and Security*(97). DOI: https://doi.org/10.1016/j.cose.2020.101959

Da Veiga, A., Ochola, E., Mujinga, M., Padayachee, K., Mwim, E., Kritzinger, E., & Machaka, P. (2021). A Reference Point for Designing a Cybersecurity Curriculum for Universities. *Human Aspects of Information Security and Assurance*. 613. DOI:10.1007/978-3-030-81111-2_5, Available at: https://uir.unisa.ac.za/handle/10500/29474

Guo, H., & Tinmaz, H. (2023). A survey on college students' cybersecurity awareness and education from the perspective of China. *Journal for the Education of Gifted Young Scientists, 11*(3), 351-367. DOI: https://doi.org/10.17478/jegys.1323423

Hnaif, A., Derbas, A., & Almanasra, S. (2023). Cybersecurity integration in distance learning: an analysis of student awareness and attitudes. *Indonesian Journal of Electrical Engineering and Computer Science, 33*(2), pp. 1057-1066. DOI: http://doi.org/10.11591/ijeecs.v33.i2.pp1057-1066

Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, pp. 1-12. DOI: https://doi.org/10.1145/3465481.3469199. Available at: https://dl.acm.org/doi/10.1145/3465481.3469199

Jayalath, J., & Premaratne, S. (2021). Analysis of Key Digital Technology Infrastructure and Cyber Security Consideration Factors for Fintech Companies. *IJRP, 84*(1), pp.128-135. DOI: 10.47119/IJRP100841920212246

ISO. (2022). *Information security, cybersecurity and privacy protection.* International Organization for Standardization. Retrieved from https://www.iso.org/standard/27001

ITU-D. (2023). *Cybersecurity Program Global Cybersecurity Index – GCIv5 Reference Model (Methodology).* Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2E.pdf

ITU. (2021). *Global Cybersecurity Index 2020.* Geneva. Retrieved from https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an Improved Understanding of Human Factors in Cybersecurity. *IEEE Humans and Cyber Security Workshop*, California. Available at: https://research.monash.edu/en/publications/towards-an-improved-understanding-of-human-factors-in-cybersecuri-2

Law No. 09-04. (2009). Official Journal of the Algerian Republic. *The specific rules for the prevention and fight against crimes related to information and communication technologies* (47). Retrieved from https://www.arpce.dz/ar/file/s0w5l9

Law No. 18-04. (2018). establishing the general rules relating to mail and electronic communications. *Official Journal of the Algerian Republic* (27). Retrieved from https://www.arpce.dz/ar/file/u6l3q2

Liu, N., Nikitas, A., & Parkinson, S. (2020). Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transportation Research Part F*, 75(4), pp. 66-86. DOI: https://doi.org/10.1016/j.trf.2020.09.019

Marican, M., Abd Razak, S., Selamat, A., & Othman, S. (2023). Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access*, 11, pp. 5442-5452. DOI: 10.1109/ACCESS.2022.3229766

Marican, M., Othman, S., Selamat, A., & Abd Razak, S. (2023). Quantifying the Return of Security Investments for Technology Startups. *Baghdad Science Journal, 21*(7). DOI: https://dx.doi.org/10.21123/bsj.2023.9077

Menasri, A. (2023). Cybersecurity Challenges in Algeria: A Comparative Study with Morocco. *Journall of Economics and Human Development, 14*(1), pp. 471-484. Retrieved from https://www.asjp.cerist.dz/en/article/227737

Mendoza, A., Roque Hernández, R., Quezada, M., & Salazar Hernández, R. (2023). Cybersecurity among University Students from Generation Z: A Comparative Study of the Undergraduate Programs in Administration and Public Accounting in two Mexican Universities. *TEM Journal, 12*(1), pp. 503-511. DOI: 10.18421/TEM121-60

Moallem, A. (2019). Cyber Security Awareness Among College Students. *Advances in Human Factors in Cybersecurity. AHFE 2018. Advances in Intelligent Systems and Computing Springer.* 782, pp. 79-87. DOI: https://doi.org/10.1007/978-3-319-94782-2_8

Moiseienko, T., & Kiva, A. (2021). Cybersecurity Startup Investments. *Cybersecurity Providing in Information and Telecommunication Systems, in Size of the cybersecurity market worldwide-Statista*. Available at: https://ceur-ws.org/Vol-3188/short6.pdf

Nelson, N., & Madnick, S. (2017). Studying the Tension Between Digital Innovation and Cybersecurity. *3rd International Conference on Information Systems Security and Privacy (SIGSEC).* Porto: Association for Information Systems. Retrieved from https://dspace.mit.edu/handle/1721.1/120720

Ng, A., & Kwok, B. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance, 25*(4), pp. 422-434. DOI: https://doi.org/10.1108/JFRC-01-2017-0013

Nobles, C. (2019). Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity. *Proceedings of the Fourteenth Midwest Association for Information Systems Conference.* Wisconsin. Retrieved from https://aisel.aisnet.org/mwais2019/22

Norval, C., Janssen, H., & Singh, J. (2021). Data protection and tech startups: The need for attention, support, and scrutiny. *Policy Internet* (13), pp. 278–299. DOI: https://doi.org/10.1002/poi3.255

Orero-Blat, M., Palacios-Marqués, D., & Garzón, D. (2021). Knowledge assets for internationalization strategy proposal. *Journal of Innovation & Knowledge, 6*(4), pp.214-221. DOI: https://doi.org/10.1016/j.jik.2020.08.002

Ozkan, B., & Spruit, M. (2023). Adaptable Security Maturity Assessment and Standardization for Digital SMEs. *Journal of Computer Information Systems, 63*(4), pp. 965-987. DOI: https://doi.org/10.1080/08874417.2022.2119442

Pollini, A., Callari, T., Tedeschi, A, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cogn Tech Work,* 24, pp. 371–390. DOI: https://doi.org/10.1007/s10111-021-00683-y

Pratomo, A. (2023). Testing the Effect of Big Data Analytics, Cybersecurity Measures, and User Training on Accounting Information System Performance in Start-up Companies in Indonesia. *West Science Business and Management*, 1(1), pp. 42-50. Retrieved from https://wsj.westscience-press.com/index.php/wsbm/article/view/381

Saoud, W., M. Meddahi (2023). A comparative analysis of the startups ecosystem in the UAE and KSA with reference to Algeria. *Economics and management*, 20(2), pp. 67-92, DOI: 10.37708/em.swu.v20i2.5

Schroth, F., & Häußermann, J. (2018). Collaboration Strategies in Innovation Ecosystems: An Empirical Study of the German Microelectronics and Photonics Industries. *Technology*

Innovation Management Review, 8(11), pp. 4-12.Available at: https://publica-rest.fraunhofer.de/server/api/core/bitstreams/fdc13f95-0119-47bf-adbb-4049fcff484e/content

Selvan, A., & Fonceca, C. (2023). Cyber security culture in an IT company: An empirical study. *International Journal of Multidisciplinary Research and Growth Evaluation, 4*(2), pp. 351-354. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4639919

Sereir El Hirtsi, H. (2023). An In-depth Study For A Proposed National Cyber Security Strategy For Digital Economy In Alegria. *Journal of Economics and Management, 23*(2), pp.12-28. Retrieved from https://www.asjp.cerist.dz/en/article/237527

Shenkoya, T., Hwang, K., & Sung, E. (2023). Student Startup: Understanding the Role of the University in Making Startups Profitable Through University-Industry Collaboration. *SAGE Open, 13*(3), pp.1-12. DOI: https://doi.org/10.1177/21582440231198601

Shun Xiang, C., & Hasbullah, M. (2023). Cybersecurity Awareness, Cyber Human Values and Cyberbullying Among University Students in Selangor, Malaysia. *International Journal of Advanced Research in Technology and Innovation, 5*(2), pp.1-11. DOI: https://doi.org/10.55057/ijarti.2023.5.2.1

Taylor-Wesselink, K., & Teulon, F. (2022). The interaction and influence of digital and non-digital structures, cultures and social norms on entrepreneurship. *Canadian Journal of Administrative Sciences/Revue canadienne des sciences de l'administration,* 39(3), pp. 244–258. DOI: https://doi.org/10.1002/cjas.1639

Zhang, T. (2020). T*hree essays on the economics of cybersecurity*. *Faculty of the Graduate College of the Oklahoma State University in partial fulfillment of the requirements for the Degree of Doctor Of Philosophy*. Oklahoma. Available at: https://scholarshare.temple.edu/bitstream/handle/20.500.12613/7982/Zhang_temple_0225E_14990.pdf?sequence=1

Zhang-Kennedy, L., & Chiasson, S. (2020). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR),* 54(1), pp.1-39. DOI: https://doi.org/10.1145/3427920

Zhang-Kennedy, L., & Chiasson, S. (2020). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys,* 54(1). DOI: https://doi.org/10.1145/3427920