International Review of Management and Marketing

ISSN: 2146-4405

available at http: www.econjournals.com

International Review of Management and Marketing, 2026, 16(5), 333-346.

Cybersecurity Awareness among Women and Youth E-commerce Entrepreneurs in Bangladesh: An Exploratory Factor Analysis

Malik Shahzad Shabbir[1]*, Fariha Karim[2], Nurul Mohammad Zayed[1], Md. Serajum Monir[3], Munmun Shabnam Bipasha[2], Friday Ogbu Edeh[4], Adeeb Alhebri[5], Mohammad Jaradat[6], Ajay Bansal[7], Laila Refiana Said[8]

[1]Faculty of Business and Communication, INTI International University, Persiaran Perdana BBN, Nilai, Negeri Sembilan, Malaysia, [2]Department of Business Administration, Daffodil International University, Dhaka, Bangladesh, [3]Faculty of Business, University of Information Technology and Sciences, Dhaka, Bangladesh, [4]Department of Research and Innovations, College of Economics and Management, International University (Main Campus), Kampala International University (Main Campus), Uganda, [5]Accounting Program, Applied College at Muhyle, King Khalid University, Abha, Kingdom of Saudi Arabia, [6]Bogdan Vodă University, Cluj-Napoca, Napoca, Romania, [7]Jaipuria Institute of Management, Noida, Uttar Pradesh, India, [8]Universitas Lambung Mangkurat, Banjarmasin, Indonesia. *Email: malikshahzad.shabbir@newinti.edu.my

Received: 27 February 2026 **Accepted:** 30 May 2026 **DOI:** https://doi.org/10.32479/irmm.23988

ABSTRACT

The issue of cybersecurity has taken the center stage among e-commerce business people especially in developing nations where the level of digital adoption is growing fast, with little awareness. This paper examines the hidden facets of cybersecurity awareness among the women and young e-commerce entrepreneurs in Bangladesh, which promotes gender equality in entrepreneurship. A quantitative method was employed to gather data on 244 respondents using a structured survey and an analysis of the data using Exploratory Factor Analysis (EFA) through SPSS. The findings indicate that cybersecurity awareness is a multidimensional concept that consists of three crucial variables, including cybersecurity awareness and risk perception, digital literacy and security practices, and cybersecurity knowledge with training and institutional support are needed for decent work and economic growth of SME entrepreneurs. Of these, the risk perception was found to be the strongest dimension, which means that the perception of the cyber threats by entrepreneurs is one of the most influential factors that determine their security behavior. The results also indicate the need to lay emphasis on digital literacy as a tool of facilitating safe online activity, as well as identify the gaps in formal education and institutional resources. The research will add value to the current body of literature, as it offers a unified model of cybersecurity awareness in the scenario of women and youth entrepreneurship in a developing economy, all these will reduce inequalities in SME sector.

Keywords: Cybersecurity, SME, Exploratory Factor Analysis, Entrepreneurs, Digital Awareness, Economic Growth, Gender Equality
JEL Classifications: D83, L86, M15

1. INTRODUCTION

The rapid evolution of digital technologies has redefined the business operations in the entire world and small and medium-sized enterprises (SMEs) are more likely to seek customers online, streamline the operations and grow the markets. E-commerce has emerged as one of the driving forces of the economic development of the developing countries such as Bangladesh and women and young entrepreneurs are a part of the development of the industry. But, with these opportunities, the growth of online business operations has placed SMEs at risk of cybersecurity threats never seen before. Debb and Mcclellan (2021), Found that Examples of cyberattacks are phishing, malware, ransomware and data breaches, which may have a devastating effect on the finances,

operations, and reputation of these businesses. Even despite the growing dependence on digital infrastructure, many SMEs in Bangladesh are unprepared because most of them do not possess the technical knowledge, resources, and have no experience of formal training on cybersecurity (Aslam et al., 2026).

According to de Nobrega et al. (2024), the cybersecurity awareness construct has a number of dimensions, which when put together will determine how a person or a company can recognize and respond to cyber threat. Cybersecurity knowledge, digital literacy, adopting security practices, risk perception, and training and institutional support are the significant ones. These dimensions have been discovered to be interrelated: the more educated about cybersecurity, the more entrepreneurs are likely to adopt specific security measures, and the greater the opportunities to maneuver the online space in a safe way, the higher the levels of digital literacy. Moreover, the threat of cyber risks inspires people to act proactively, and formal training courses offer the guidance that is likely to help them to convert knowledge into practice.

Women and youth entrepreneurs are reduced to being vulnerable when it comes to the case of Bangladeshi e-commerce. The majority of them lack training on information technology and cybersecurity and, therefore, do not know about the threats and have limited capacity to defend themselves (Aslam et al., 2026; Nawaz et al., 2025; Mazumdar and Alharahsheh, 2019). Also, insufficient institutional support and funding contribute to the negative impact of holistic security measures implementation, which puts these entrepreneurs at risk of cyberattacks. It is an especially worrying vulnerability considering that SMEs are becoming the main targets of cybercriminals because of their seemingly weak security measures (Chotia et al., 2025).

Lasi (2025) found that the indicate that there is need to acquire knowledge and skills on cybersecurity to mitigate these risks. Bringing awareness of popular cyber threats, safe online habits, and a post-hack impact to entrepreneurs would enable knowledgeable decision-making and proactive behavior. Digital literacy programs such as privacy settings training, secure transactions and use of digital tools support the adoption of cybersecurity practices directly. Similarly, institutional support and formal training play a crucial role in creating an enabling environment that enables the access of entrepreneurs to guidance, technical support, and practical resources to help ensure their digital operations are secure.

Although these understandings, scanty empirical data exists regarding the particular aspects of cybersecurity awareness among women and youth e-commerce entrepreneurs in Bangladesh. These latent factors are important to understand in order to develop effective interventions to meet the special needs of this group of people. Corradini and Nardelli (2020) found that the latent constructs of cybersecurity awareness taking into consideration five variables, namely cybersecurity knowledge, digital literacy, security practices, risk perception and training and institutional support. With these factors in place, the study will possess a holistic framework that can be utilized to educate the policymakers, training institutions and development agencies on the ways of enhancing cybersecurity preparedness among the resource limited SMEs.

Lastly, this study is also a contribution to the current body of research on cybersecurity in developing economies. Zwilling et al. (2022) indicates how awareness is multidimensional and the importance of knowledge and digital skills, risk perception, and institutional support in the decision-making on secure online behavior. The results have real-world applications in enhancing the resilience of e-commerce businesses, especially those that are run by women and the youth, in the face of the constantly changing environment of cybercrimes in Bangladesh.

This paper looks into the complex structure of cybersecurity awareness among women and youth e-commerce entrepreneurs in Bangladesh. Therefore, the study seeks to answer the research questions:

RQ1: What are the latent factors of cybersecurity awareness among female and young e-commerce entrepreneurs in Bangladesh?

RQ2: What are the cybersecurity knowledge, digital literacy, cybersecurity practices, cybersecurity risk, and training and institutional support of women and youth e-commerce entrepreneurs in Bangladesh?

2. LITERATURE REVIEW

Cybersecurity is a developing issue in SMEs more so as they continue to depend on digital technologies. Lack of resources, knowledge, and expertise in cybersecurity practices make many SMEs susceptible to cyberattack (Isa et al., 2026). As is witnessed in researches carried out on European SMEs, absence of IT security puts these enterprises at risk of cybercrimes which include phishing, malware and ransomware. SMEs are not always organized with their cybersecurity, where the management fails to invest funds in securing their online infrastructure. This is especially important to women and young entrepreneurs in the e-commerce industry in Bangladesh where the lack of resources and awareness is an additional factor that increases vulnerabilities Studies have shown that awareness of employees and the management on cybersecurity matters is critical in averting cyber threats. In SMEs, especially in developing countries, there is a general lack of training and education on cybersecurity risks. This ignorance especially among women-based and youth-based e-commerce companies is usually translated to the use of poor security measures thus such companies are easy targets of cybercrime (Chowdhury et al., 2023). Research has indicated that cybersecurity education is capable of lowering the chances of cyberattacks by a considerable margin by raising the awareness of the employees on the possible threats and the significance of secure digital behaviors (Zwilling et al., 2022).

One of the issues facing SMEs, such as e-commerce businesses, is the rising level of sophistication of cyber threats. SMEs are often vulnerable to cybercriminals because their vulnerability is perceived by cybercriminals, particularly when they are not adequately funded to ensure cybersecurity Adriko and Nurse (2026). Phishing and computer fraud along with malicious software are highly common in SMEs, which are perilous. These

risks are especially vulnerable to e-commerce entrepreneurs, particularly women and the young in Bangladesh, where digital adoption is growing fast. Without proper cybersecurity practices, these businesses face the possibility of data breaches, financial fraud, and brand reputation damage.

The female and young entrepreneurs in Bangladesh lead in the development of e-commerce but are less knowledgeable on the dangers of cyber security. This group is very susceptible because of the lack of exposure to formal training in IT and cybersecurity. Awareness campaigns, workshops, and designing user friendly cybersecurity tools can be used to empower these entrepreneurs to protect their businesses against cyber threat Chaudhary et al. (2023). These initiatives will mitigate the threat of cybercrime in this vital part of the Bangladesh economy by meeting the unique needs and challenges of women and youth entrepreneurs.

2.1. Cybersecurity Knowledge and its Impact on SMEs

Within the context of SMEs, e-commerce businesses included, cybersecurity awareness is a key catalyst to encourage proactive risk management. Research conducted on SMEs in Malaysia revealed that cybersecurity knowledge is the best predictor of cybersecurity awareness, which underscores its inherent importance in influencing attitudes and behavioral tendencies towards cyber threats (Abdul Lasi, 2025). This is in line with the findings that SMEs remain unprepared to cyberattacks, in large part, because of the lack of knowledge and awareness about the risks involved (Adriko and Nurse, 2026). Cybersecurity awareness in e-commerce is most often inadequate among women and youth entrepreneurs, thus exposing their businesses to vulnerabilities. Their ignorance about cybersecurity leads to the SMEs ignoring security or being unaware of the entire scope of cybersecurity risks, such as phishing, malware, and ransomware. This is of particular concern to women and young entrepreneurs who may lack formal training in IT and cybersecurity, and thus, are more vulnerable to cyberattacks (Chotia et al., 2025).

Studies have highlighted that cybersecurity awareness can only be improved by enhancing cybersecurity knowledge. In the case of SMEs, the knowledge gap can be narrowed by raising awareness via training sessions, workshops, and available resources and mitigating cyber threats associated risks (Vladimirovna and Zayed, 2021, Gazi et al., 2025). Also, cybersecurity expertise can enable entrepreneurs to realize the necessity of investing in cybersecurity even with limited resources (von Solms and van Niekerk, 2013; Rehman et al., 2024). This result is in line with the necessity of specific cybersecurity education of women and youth e-commerce entrepreneurs, which can result in more knowledgeable decision-making and improved data security (Aslam et al., 2026). The study also reveals a gap in cybersecurity knowledge by SMEs. Cybersecurity is an area that is taken lightly by many SME owners, especially in developing countries such as Bangladesh, who do not have the knowledge on the risks involved. This ignorance results in a reactive but not a proactive response to cybersecurity with most businesses responding to a cyberattack when it has already taken place. This is a severe problem to women and youth entrepreneurs in Bangladesh because they might not emphasize cybersecurity information until they are impacted, which can hurt their businesses (Adriko and Nurse, 2026).

The study also briefly mentions cyber insurance as a supplementary mechanism of dealing with cyber risks as most SMEs including e-commerce business feel no need to have it because they lack knowledge on cybersecurity. This is in line with the notion that cyber insurance can only be of value when it is required by clients or regulators. Lack of adequate knowledge about cybersecurity can lead SMEs to the inability to see how cyber insurance fits into their risk management plans (Adriko and Nurse, 2026, Mia et al., 2022).

Female and young entrepreneurs in Bangladesh are not typically trained on IT and cybersecurity, which increases their susceptibility to cyberattacks. These entrepreneurs might be unaware of possible risks or fail to take the required security precautions without adequate cybersecurity knowledge, exposing them to greater cyber threats. This ignorance is especially alarming since it is to this group of SMEs that cybercriminals focus their attention since they have weak defenses (Chaudhary et al., 2022).

2.2. Digital Literacy in Cybersecurity Awareness Role

The digital literacy aspect plays a significant role in enhancing cybersecurity awareness, particularly among the underrepresented groups, such as women and youth entrepreneurs. According to digital literacy involves a spectrum of skills, including the simplest ones such as computer use, and more sophisticated ones such as internet-safety and control over digital devices. This interpretation of online spaces has a considerable effect on the capacity of the person to identify cyber threats and engage in protective actions .

According to a study by, digital literacy does not only concern the skills related to the technical aspect but also the awareness of the risks on the Internet and the understanding of how to avoid them. When applied to women and youth entrepreneurs, particularly in e-commerce, digital literacy helps them to have a more effective control of their business online and prevent various risks, including phishing, identity theft, and malware. An entrepreneur can be more or less digitally understanding, and the more digitally understanding the entrepreneur is, the more likely he/she will understand the necessity of cybersecurity and take precautions to safeguard their online activities.

The study by Estrada et al. (2022) indicates that the digital literacy of an individual has a direct relationship with the capability to take part in cybersecurity practices. More digitally literate entrepreneurs will also tend to engage in safe online behaviors, such as antivirus software use, safe browsing, and sensitive data protection. Such practices are essential in e-commerce companies where confidential information of customers is regularly shared over the internet. Through developing digital literacy, entrepreneurs are more equipped to find their way in the digital world safely and securely with reduced vulnerabilities in their online business processes.

Moreover, emphasize that disadvantaged populations, especially women, experience further obstacles to becoming digitally literate, which further increases their susceptibility to cyberattacks. This paper proposes the idea that special training sessions based on digital literacy and cybersecurity could help these entrepreneurs to be more security conscious and less vulnerable to cyberattacks.

Digital literacy education bridges the knowledge gap and encourages a more active approach to dealing with cybersecurity threats (Estrada et al., 2022).

2.3. Security Awareness and Practices

Security practices are essential for safeguarding businesses against cyber threats. Due to a weak level of security measures, SMEs such as e-commerce businesses are prone to higher risks. Studies indicate that firewalls, encryption, and frequent updates of systems are some of the security measures that can ensure digital assets and sensitive information are safeguarded. When these practices are not adhered to, women and youth entrepreneurs are especially vulnerable since they might not have formal training in IT (Iqbal et al., 2021). By ensuring that SMEs implement these security practices, they will be less susceptible to cyberattacks such as data breaches, malware attacks, and denial of service attacks (Chidukwani et al., 2022). Good security practices can help to create resilience within organizations (Germanos et al., 2026). According to, the more organizations learn on how to respond to previous cybersecurity attacks and modify their security responses, the more resilient they become to the attacks in the future. The adoption of security practices in the daily business activities enables SMEs to improve their ability to detect, prevent, and respond to cyber threats (Ainslie et al., 2023). In Bangladesh, this stands as one of the most effective protective measures against cyber incidents since women and young entrepreneurs would not only be reducing the risk of these events but also enhancing their business stability in general in a digital world that is constantly becoming vulnerable to cyberattacks.

Security practices and cybersecurity knowledge will be linked (Ruohonen et al., 2025). Although security practices are much needed, a considerable number of SMEs, particularly those operated by women and youth, are hindered by various obstacles in implementing them. Limited resources, knowledge, and time may make it unfeasible to implement the holistic security measures in the business. Although SMEs usually understand the significance of security practices, they do not have sufficient funds and lack the knowledge to use these practices to the fullest (Erdogan et al., 2023). This especially applies to women and young business owners who, possibly, lack technical skills to install a strong security system and hence are more susceptible to cybercrime (Patterson et al., 2024). Security practices are introduced to many SMEs with the help of the external support of IT companies or consultants. Emphasise that IT companies are instrumental in offering advice and resources to the SMEs on the best security practices. This is particularly significant to women and young business people who might not possess in-house IT knowledge. With the help of external support, entrepreneurs are able to take security measures that would prevent their businesses to be subjected to cyber risks and to make sure that they meet the industry standards (Suhail et al., 2025).

2.4. Risk Perception and Cybersecurity Awareness

One of the key ideas in explaining cybersecurity behavior is risk perception, especially in women and youth entrepreneurs in e-commerce where human decision-making is a key factor in determining security (Debb and Mcclellan, 2021). Risk perception is subjective perception of the risk severity and likelihood by an individual that affects precautionary behavior and adherence to security measures.

The studies show that perceived vulnerability is a major factor that influences cybersecurity behavior. Also note that people who feel more vulnerable to the threat of cybercrime tend to implement protective practices (van Schaik et al., 2017). Protection Motivation Theory (PMT) is a theory that indicates that the behavioral intentions are influenced by both threat appraisal and coping appraisal, and threat appraisal includes the assessment of the severity and personal susceptibility, and coping appraisal includes self-efficacy and response efficacy (Menard et al., 2017). Precautionary measures are further justified by exposure to previous cyber-attacks that increase perceived vulnerability.

The empirical research on the educational setting has revealed that risk perception of students differs among various cyber hazards (Alam et al., 2025). Perceived risk was found highest when it comes to identity theft, social engineering, and cyberbullying, and other factors that are important in predicting precautionary behavior include voluntariness, immediacy, dread, and perceived control (Sagita et al., 2025; Ng et al., 2025). Likewise, affective reactions affect the perception, as people tend to relate activities to positive emotions, which results in risk underestimation (Kostyuk and Wayne, 2021).

In small and medium enterprises (SMEs), it is especially important as the lack of resources and awareness increases vulnerability (Ashley and Preiksaitis, 2022). SMEs tend to overestimate their cybersecurity risks, leading to a lack of adequate measures to safeguard against cybercrimes (Panko et al., 2025). Research indicates that training, awareness campaigns, and a strong security culture are essential in creating risk perception and enhancing compliance. Moreover, gamified learning systems like CySecEscape were found to increase awareness and change the perception of risk, resulting in a more proactive approach (Boopathi et al., 2015).

2.5. Training and Institutional Support and Cybersecurity Awareness

Institutional support and training are also vital in making people and organizations more aware of cybersecurity and increase protective measures (Ahmad Zukarnain et al., 2020). Studies emphasize that the level of cybersecurity threats is getting more advanced, and the knowledge, skills, and active involvement of employees are in the spotlight in averting the risks. Education programs, especially the ones that are ongoing and organized, can help create a cybersecurity-aware workforce that can help in stopping and reacting to cyber-attacks (Khan et al., 2025).

As empirical evidence shows, structured training programs have a positive impact on the amount of knowledge, attitude, and behavior about cybersecurity (Abukeshek et al., 2026). Knowledge-Attitude-Behavior (KAB) model suggests that better knowledge acquisition in the form of training may result in attitudinal change and, finally, behavioral change, which will support organizational security practices (Oakley Browne and Pardede, 2026). Systematic

awareness programs, adjusting to organizational settings, like the Cybersecurity Awareness Training Model (CATRAM), have also been demonstrated to benefit the effectiveness of the training process as they focus on the specific roles and perception of threats among organizations (Sabillon et al., 2019, Prada et al., 2023).

Besides training, knowledge exchange, and peer support have been identified as critical tools of maintaining cybersecurity awareness. As shown in the Transitive Memory System (TMS) framework, employees can enhance organizational security knowledge through informing employees on what they should know, as well as through sharing expertise (or knowledge) collectively, which complements formal training initiatives (Arsenovych et al., 2024). Sharing security knowledge will help increase the confidence of employees and makes the practice of cybersecurity more practical, especially in the context of SMEs, where resources are a limited resource (Khan et al., 2025; Ng et al., 2025).

SMEs particularly need training and support, as financial limitations, lack of technical skills, and insufficient institutional support often restrict the level of cybersecurity capabilities. Research shows that SMEs often do not adequately consider their exposure to cyber risks, which poses the significance of tailored training and advisory services to enhance awareness as well as proactive defensive practices (Khayer et al., 2021). SMEs training does not only enhance the technical skills but also enhances decision making and risk management in their day-to-day operations.

Moreover, the development of digital technologies has made it possible to implement more efficient and interactive training methods, such as remote labs, gamified learning, and simulators (Sas et al., 2021) These strategies increase learning engagement, reinforcement, and offer real-world and practical experiences to the participants to increase the retention and utilization of cybersecurity education (Alahmari et al., 2023) (Table 1).

3. RESEARCH METHODOLOGY

This research follows a quantitative research methodology to explore the underlying factors of cybersecurity awareness among young and female e-commerce entrepreneurs in Bangladesh. Primary data were collected using a structured survey, enabling statistical processing and generalization of results.

3.1. Research Design

A cross-sectional study design was adopted, in which data were collected at one specific point in time from respondents involved in e-commerce. This type of design is suitable for uncovering patterns, associations, and factors associated with cybersecurity awareness.

3.2. Sampling Technique and Sample Size

The research subjects were e-commerce entrepreneurs in Bangladesh, focusing on women and youth. A non-probability sampling method, convenience sampling, was used for the study due to accessibility and time. The researchers gathered 244 eligible responses for analysis, which is satisfactory for factor analysis. The study used a questionnaire with a number of items rated on a Likert scale (e.g., 1 = Strongly Disagree to 5 = Strongly Agree).

3.3. Data Analysis Techniques

We used the Statistical Package for the Social Sciences (SPSS) to analyze the data. The main method used was Exploratory Factor Analysis (EFA) to determine the factors of cybersecurity awareness.

Before conducting EFA, the suitability of the data was assessed using:

- Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy
- Bartlett's Test of Sphericity.

Principal Component Analysis (PCA) with Varimax rotation was used to extract factors. Factors with eigenvalues >1 were selected and items with substantial factor loadings were clustered.

4. DATA ANALYSES

The age distribution of the respondents indicates that a large percentage of e-commerce entrepreneurs involved in the study are young with 95.08 (232 of 244) being between the age group of 18 and 24 years. Only a very small percentage, 4.91% (12 respondents) falls in the age bracket of 25-30 years. This means that women and youth entrepreneurship in the Bangladeshi e-commerce industry is highly characterized by very young adults, which implies the high presence of individuals in early career in advancing digital business activities.

The educational level of the respondents shows that the majority of the women and youth e-commerce entrepreneurs in the research have a bachelor degree which makes up 86.05% (210 of 244) of the sample. A lesser percentage holds a diploma (12.70%, 31 respondents), and 1.22% (3 respondents) hold a master degree. This implies that most business owners have a relatively high level of education, which could be helpful to them in their digital business operations, although higher education (masters) is uncommon among them.

Out of 244 respondents, most women and youth e-commerce entrepreneurs are involved in the clothing and apparel industry (33.60%), IT and software companies (14.34%), electronics and gadgets (13.52), and handicrafts or homemade products (12.70). Food and drinks businesses take 10.65% and restaurants and cafes 11.47, furniture manufacturing and grocery shops constitute a very insignificant percentage (1.63 and 2.04, respectively). This dispersion puts emphasis on the fashion, technology and creative home based businesses in the youth dominated e-commerce in Bangladesh.

Business Experience: The majority of the respondents are not very experienced entrepreneurs with 72.54% of all having <1 year of business experience. Individuals who have 12 months to 2 years of experience make 20.49, 3-5 years' experience makes 5.32 and there are only 1.63 years of experience. This means that this sector is characterized by early-stage entrepreneurs, which show a high rate of young people joining the digital market.

Table 1: Summary of studies on risk perception in cybersecurity

Focus Study	Authors	Key Findings
Cybersecurity Knowledge	Lasi (2025)	The best predictor of cybersecurity awareness is cybersecurity knowledge, which influences attitudes and behavior towards cyber threats.
	Adriko & Nurse (2026)	Knowledge deficit results in insufficient planning and responsive strategies toward cybersecurity.
	Akter et al. (2025)	A lack of cybersecurity awareness makes it easier to be the prey of phishing, malware, and ransomware.
	Akter et al. (2025)	Specific training enhances the knowledge, and the entrepreneurs can undertake security measures even in cases where resources are limited.
Digital Literacy	Dodel & Mesch (2018)	Online literacy improves capacity to perceive cyber risks and embrace safety measures.
	Rocha Estrada et al. (2022)	Online risk awareness and safe business practices are enhanced by digital literacy.
	Ahammed et al. (2024)	The increased digital literacy is associated with the adoption of secure online behaviors; targeted training has the greatest impact on the underrepresented groups.
Security Practices	Badghish & Soomro, (2024)	Digital literacy is a predictor of safe behaviours such as phishing detection and safe online behaviours.
	Patterson et al. (2024)	Incorporation of security practices into the organization increases resilience against cyber threats.
	Ainslie et al. (2023)	Informed business persons embrace major security measures like password management, safe transactions, and training of employees.
	Becker & Schmid, (2020)	The absence of resources and knowledge blocks the implementation of security measures; the external IT assistance is essential, particularly to women and youth entrepreneurs.
Risk Perception	Elhusseiny & Crispim, (2021);	The perceived severity and probability of threat affect precautionary behaviour and adherence.
	Debb & McClellan (2021); Thakur & Alam (2022)	The behavioral intentions are determined by threat and coping appraisal (Protection Motivation Theory).
	Kostyuk & Wayne (2021); Techanamurthy (2025); Veksler et al. (2018)	Pre exposure to cyber incidents leads to heightened perceived vulnerability, which improves protective behavior.
	Van Schaik et al. (2017); Yuwono et al. (2024) Hossain et al. (2023); Islam et al. (2009); Shahzad (2023)	The perceived risk was greatest with identity theft, social engineering, cyberbullying; variables such as voluntariness and dread are predictors of precautionary behavior.
	Panko et al. (2025); Hossain et al. (2025); Islam et al. (2025)	Few resources make one more vulnerable; gamified tools such as CySecEscape enhance risk perception.
	Ashley & Preiksaitis (2022); Hirvonen & Majuri (2020); Kabir & Reem (2025); Shahadat et al. (2023)	Risk perception and compliance is enhanced through training, awareness programs and good security culture.
Training & Institutional Support	Zukarnain et al. (2020); Häring (2025); Kanbacha et al. (2024)	Ongoing, formal training enhances the sensitization and defensive practices.
	Sas et al. (2021); Haque et al. (2024); McCrohan et al. (2010); Santos et al. (2024)	Systematic training enhances knowledge, attitudes, and behavior related to cybersecurity (KAB model).
	Sabillon et al. (2019); Haq & Huo, (2023); Mia et al. (2022);	CATRAM model demonstrates that role-specific and threat-perception-based tailored training enhances effectiveness.
	Alahmari et al. (2023); Gold (2025); Mogaji et al. (2024); Rupa et al. (2026)	The Transactive Memory System (TMS) strategy improves the exchange of knowledge, which strengthens the results of training.
	Khan et al. (2025); Ghobakhloo et al., (2022); Nishu et al. (2025); Rahman & Majumder (2020)	Low cybersecurity ability SMEs are offered advisory support and training; training enhances skills, decision-making, and risk management.
	Prada et al. (2023); Arsenovych et al. (2024); Ntlatlapa (2023); Prasanna et al. (2019)	Remote labs, gamified exercises, and simulation platforms enhance engagement, knowledge retention, and practical application of cybersecurity skills.
	Browne & Pardede (2026); Pandya (2012); Pavlova et al. (2021)	Training programs enhance the level of technical skills, risk awareness and confidence, which are vital in resource-constrained SMEs.

Table 2: Demographic analyses

Variable	Age	Count	Percentage
Age	18-24 years	232	95.08
	25-30 years	12	4.91
	Total	244	100
Level of education	Bachelors	210	86.05
	Diploma	31	12.70
	Total	244	100
Business type	Clothing/Apparel	82	33.60
	Electronics/Gadgets	33	13.52
	Food and Beverage	26	10.65
	Furniture manufacturing	4	1.63
	Grocery shops	5	2.04
	Handicrafts/Homemade Products	31	12.70
	IT and software firms	35	14.34
	Restaurants and cafes	28	11.47
	Total	244	100
Years of business experience	1-2 years	50	20.49
	3-5 years	13	5.32
	<1 year	177	7254
	More than 5 years	4	1.63
	Total	244	100
Type of online platform used	E-commerce marketplace (Daraz, AjkerDeal, etc.)	14	5.73
	Social Media Platform (Facebook, Instagram)	209	85.65
	website/App	21	8.60
	Total	244	100

Table 3: Reliability statistics

Reliability statistics	
Cronbach's Alpha	**N of Items**
0.961	20

Most of the women and youth e-commerce business owners examined in the research use social media, and 85.65% (209 of 244) utilize Facebook, Instagram, or other websites to conduct business. Only a few (8.60%, 21 respondents) of them use their own websites or applications, and only 5.73% (14 respondents) use existing e-commerce marketplaces, including Daraz or AjkerDeal. This indicates that the prevailing channel to reach customers and do online business among young entrepreneurs in Bangladesh is social media probably because of its availability, affordability and high number of users (Table 2).

The reliability test in Table 3 indicated that the 20-item scale had a Cronbach alpha of 0.961 which indicated a high internal consistency. This indicates that the items were very similar in the measures of the same construct. According to Tavakol and Dennick, 2011, the alpha value if is more than 0.95, and thus, an item redundancy can also occur, i.e. an item can be too similar to another.

Kaiser-Meyer-Olkin (KMO) measure and Bartletts Test of Sphericity are used to establish the appropriateness of a dataset to exploratory factor analysis (EFA). KMO statistic evaluates the extent of the commonality of the variables, whether the correlations are tight enough to extract factors. A value of 0.6 or less indicates that the data may not be sufficient to run factor analysis which yields discrete and satisfactory factors, whereas

Table 4: KMO and Bartlett's test

KMO and Bartlett's test		
Kaiser-Meyer-Olkin measure of sampling adequacy		0.957
Bartlett's test of sphericity	Approx. Chi-square	4204.521
	df	190
	Sig.	0.000

Table 5: Communalities of factors

Communalities	Initial	Extraction
Cybersecurity Knowledge 1	0.452	0.458
Cybersecurity Knowledge 2	0.743	0.757
Cybersecurity Knowledge 3	0.612	0.662
Cybersecurity Knowledge 4	0.585	0.604
Digital Literacy 1	0.657	0.632
Digital Literacy 2	0.704	0.672
Digital Literacy 3	0.696	0.662
Digital Literacy 4	0.588	0.589
Security Practices 1	0.752	0.760
Security Practices 2	0.684	0.679
Security Practices 3	0.713	0.692
Security Practices 4	0.650	0.657
Risk Perception 1	0.772	0.772
Risk Perception 2	0.750	0.725
Risk Perception 3	0.797	0.770
Risk Perception 4	0.784	0.768
Training and Institutional Support 1	0.414	0.367
Training and Institutional Support 2	0.724	0.724
Training and Institutional Support 3	0.781	0.733
Training and Institutional Support 4	0.741	0.706

Extraction Method: Principal Axis Factoring

a value of 1.0 or above indicates that factor analysis will yield discrete satisfactory factors. The test by Bartlett measures the difference between the correlation matrix and an identity matrix; a significant value (P = 0.05) indicates that variables have adequate number of correlations to warrant factor analysis (Tobias and Carlson, 1969).

According to Table 4, the Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy of 0.957 shows that the sample is very appropriate to carry out a factor analysis because a value of 0.9 and above is excellent. Besides, the Test of Sphericity by Bartlett has a significant P = 0.000 which shows that the correlation matrix is not an identity matrix, which means that there are enough relationships between variables to make factor analysis to be suitable.

It is based on the communality values to determine the extent to which each of the observed variables can be explained by the factor model. This will assist researchers to make decisions on whether the model is modeling the data adequately and whether to drop some variables because of weak or inadequate relationships with the factors extracted. The communalities may assist in determining whether to hold or dispose things depending on their input to the factors. The method of extraction applied in this analysis is Principal Axis Factoring (PAF) which is commonly applied in situations where the data is believed to be continuous and when one wishes to determine latent factors. The values of Table 5 in the communalities indicate the percentage of variation that each observed variable can be explained by the extracted factors. Above 0.5 is a typically desirable communality since it indicates that a

large percentage of the variance can be attributed to the factors (de Winter and Dodou, 2012).

The results of the factor analysis bring in the understanding of the manifestation of various facets of cybersecurity awareness and practices among women and youth e commerce entrepreneurs in Bangladesh. These variables were tested to appreciate how they contributed to latent constructs dealing with cybersecurity preparedness.

Cybersecurity Knowledge 2 is the level of awareness of entrepreneurs about the significance of securing customer data in online business setting. This variable has a high extraction value of 0.757; this implies that over 75% of the variance in this variable is captured by the extracted factors. This indicates that women and youth entrepreneurs in Bangladesh who are in e commerce who also show a good appreciation of the importance of data protection in fostering customer confidence and survival of the business.

Training and Institutional Support 1 is the type of training or formal education with regard to cybersecurity or online safety. This value of extraction (0.367) implies that the factor structure moderately explains this variable. It means that even though these entrepreneurs have taken some training, it might not be thorough and extensive enough. The cybersecurity capacity of this group may be improved by enhancing institutional support and targeted cybersecurity training programs.

Risk Perception 3 is the perception that absence of cybersecurity awareness poses more risks to business. The extraction value is 0.770, which indicates that most of the variance of this variable is explained by the latent factors. This implies that women and youth e commerce entrepreneurs in Bangladesh have a high awareness of the risk of poor cybersecurity awareness like loss of money, reputation, and interference with operations.

Security Practices 1 deals with the use of basic cybersecurity measures, including the use of secret and strong online account passwords. This variable has a large value of extraction (0.760) indicating that a large percentage of the variance is associated with the extracted factor structure. This indicates that many of these entrepreneurs are adopting critical cybersecurity measures, which form the basis of reducing typical threats such as unauthorized accession.

Factor analysis uses a scree plot to visually estimate the number of factors to be retained. It assists in determining the "elbow-point" at which the eigenvalues begin to flatten (Ledesma et al., 215) (Figure 1). The factors that have an eigenvalue larger than 1 are significant and the scree plot assists in determining which of the factors would be included in the final model by revealing where the variance contribution decreases significantly.

The first factor comprises the essence of the data in the survey, which is "Cybersecurity Awareness." This factor has the largest eigenvalue (~12), implying that it yields the greatest amount of variance. This consideration may be a combination of responses on cybersecurity awareness and knowledge of cyber risk. The second factor, which explains the lesser variance, is associated with digital literacy, which includes such skills as managing privacy settings and using online payment systems. The third factor is associated

Table 6: Factor matrix

Factor matrix	Factor		
	1	2	3
Security Practices 1	0.851		−0.183
Risk Perception 1	0.839	−0.254	
Cybersecurity Knowledge 2	0.831		0.254
Training and Institutional Support 2	0.824	−0.208	
Risk Perception 4	0.819	−0.311	
Security Practices 3	0.818	−0.111	
Risk Perception 3	0.815	−0.321	
Training and Institutional Support 3	0.815	−0.259	
Risk Perception 2	0.793	−0.280	0.133
Security Practices 4	0.790		−0.182
Training and Institutional Support 4	0.784	−0.303	
Security Practices 2	0.779	0.133	−0.234
Digital Literacy 1	0.769	0.200	
Digital Literacy 3	0.762	0.270	
Digital Literacy 2	0.758	0.308	
Cybersecurity Knowledge 3	0.700	0.178	0.375
Digital Literacy 4	0.682	0.333	−0.113
Cybersecurity Knowledge 4	0.619	0.437	0.173
Cybersecurity Knowledge 1	0.507	0.185	0.408
Training and Institutional Support 1	0.447	0.344	−0.222
Extraction Method: Principal Axis Factoring.			

[a]3 factors extracted. 6 iterations required

Extraction was conducted using Principal Axis Factoring (PAF) with Varimax rotation. Factor loadings ≥ .50 were considered practically significant. Values represent standardized factor loadings of observed variables on the extracted factors. Cross-loadings were evaluated, and items were retained based on theoretical relevance and loading strength. N = 244.

Table 7: Rotated factor matrix

Rotated factor matrix	Factor		
	1	2	3
Risk Perception 3	0.810	0.226	0.251
Risk Perception 4	0.808	0.255	0.222
Risk Perception 1	0.788	0.335	0.197
Training and Institutional Support 4	0.777	0.238	0.214
Training and Institutional Support 3	0.768	0.270	0.266
Risk Perception 2	0.760	0.191	0.334
Training and Institutional Support 2	0.744	0.348	0.220
Security Practices 3	0.678	0.436	0.206
Security Practices 1	0.602	0.597	0.202
Security Practices 4	0.570	0.551	0.171
Digital Literacy 4	0.277	0.653	0.294
Digital Literacy 2	0.345	0.650	0.363
Digital Literacy 3	0.376	0.647	0.320
Security Practices 2	0.491	0.642	0.160
Training and Institutional Support 1	0.105	0.586	0.110
Digital Literacy 1	0.425	0.569	0.358
Cybersecurity Knowledge 3	0.363	0.307	0.660
Cybersecurity Knowledge 1	0.217	0.186	0.613
Cybersecurity Knowledge 2	0.554	0.361	0.566
Cybersecurity Knowledge 4	0.140	0.534	0.547
Extraction Method: Principal Axis Factoring. Rotation Method: Varimax with Kaiser Normalization.			

[a]Rotation converged in 6 iterations

Extraction method: Principal Axis Factoring (PAF). Rotation method: Varimax with Kaiser Normalization. Rotation converged in 6 iterations. Factor loadings represent the correlations between observed variables and the extracted latent factors after orthogonal rotation. Items with factor loadings of .50 or greater were considered significant and retained for interpretation. Each item was assigned to the factor on which it demonstrated the highest loading, while cross-loadings were evaluated to ensure construct distinctiveness. N = 244.

with security behaviors, such as strong passwords and two-factor authentication. The other factors are the perception of risk and the necessity of training and institutional support, which have a very small contribution to the variance. To sum up, the most important factor is the first one, whereas the remaining ones are more specific themes with less influence on the overall variance.

A Factor Matrix is a Table 6 indicating the loadings (correlations) of individual variables (survey questions) on the extracted factors, in a factor analysis. These loadings show how strong the relationship between each of the variables and the underlying factors is. The loading is greater the stronger the relationship between the variable and the factor. The structure of the data is interpreted in the framework of the identified factors using the matrix.

The Factor Matrix contains the factor loadings of three extracted factors, which are the result of Principal Axis Factoring (PAF). The factor analysis revealed three key factors related to cybersecurity awareness (de Winter and Dodou, 2012). Factor 1, which is named Cybersecurity Knowledge and Practices, had the most significant variance, with an eigenvalue of 12, indicating the knowledge of the respondents about cybersecurity threats, security practices, and risk perceptions. Factor 2 is called Digital Literacy and measures the confidence and ability of the respondents to use digital platforms in a safe manner with the loadings of 0.758 to 0.769 on the corresponding questions. Factor 3 pertains to Training and Institutional Support that reflects the significance of training and external resources to increase cybersecurity awareness, and the loading of this factor is 0.447 and 0.344. These aspects underscore the dimensions of cybersecurity awareness that are important such as knowledge, digital skills and support structures.

The result of a factor analysis is a Factor Matrix that has gone through a rotation procedure to enhance the interpretability of the factors. In factor analysis, the aim is to simplify the data by determining the underlying factors that are associated with the variance in the variables observed. The first step is to extract factors, whose loadings (how strong the relationship between variables and factors) can be hard to interpret (Goretzko et al., 2021).

Factor rotation is used so that the interpretation is made easier. Varimax (orthogonal rotation) and Promax (oblique rotation) are the most popular forms of rotation. Varimax is designed to maximize the variance of squared loadings of each factor and hence it is less difficult to find out which variables load most onto each factor. The process aids in clarifying the factor structure and making it more distinct. Factor 1, which has the highest amount of variance is associated with cybersecurity awareness and risk perception. It demonstrates that those who are aware of cybersecurity risks (e.g., Risk Perception 3, 4 and 1) tend to take proactive action more. The reason also makes a point that training and institutional support (Training and Institutional Support 4 and 3) is important in increasing awareness on cybersecurity. Also, risk-conscious users are more likely to have better security habits, including using a strong password and data backup (Table 7).

Factor 2 is associated with digital literacy and digital security practices. It demonstrates that more digitally literate respondents (e.g., controlling privacy settings and online transactions) are more likely to adopt good security practices, including two-factor authentication and data regular backups. This connection is supported by high loadings of Digital Literacy 4, Digital Literacy 2 and Digital Literacy 3.

Factor 3 highlights the importance of cybersecurity knowledge and the role of training and institutional support. It demonstrates that respondents that have more knowledge about cybersecurity threats (e.g., Cybersecurity Knowledge 3, 1, and 2) have a higher score on this factor. Also, training and institutional support (e.g., Training and Institutional Support 1 and 2) play an important role in enhancing the knowledge and improving cybersecurity practices.

The Factor Transformation Matrix in Table 8 shows how the extracted factors (before rotation) are transformed into the rotated factors (after applying Varimax rotation). It provides the relationship between the original factors and the rotated factors, which helps in interpreting the factors more clearly (Weide and Beauducel, 2019).

Factor 1 from the original factors has a strong correlation with rotated Factor 1 (0.728) and a moderate negative correlation with rotated Factor 2 (−0.683), indicating that it primarily contributes to rotated Factor 1, but also has a slight negative relationship with rotated Factor 2.

Factor 2 from the original factors is moderately correlated with rotated Factor 1 (0.556) and strongly correlated with rotated Factor 2 (0.643), suggesting it contributes more significantly to rotated Factor 2.

Factor 3 has a very weak negative correlation with rotated Factor 1 (−0.065) and a moderate negative correlation with rotated Factor 2 (−0.526), meaning it has a minor contribution to rotated Factor 1 but plays a more notable role in rotated Factor 2.

Table 8: Factor transformation matrix

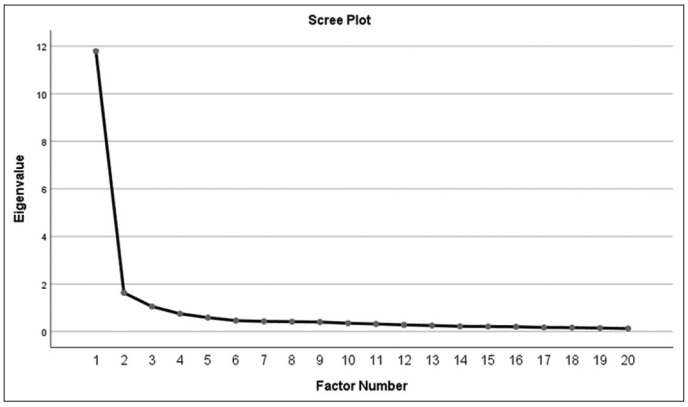
Factor transformation matrix			
Factor	**1**	**2**	**3**
1	0.728	0.556	0.401
2	−0.683	0.643	0.347
3	−0.065	-0.526	0.848

Extraction Method: Principal Axis Factoring. Rotation Method: Varimax with Kaiser Normalization

5. FINDINGS

The Factor Transformation Matrix of factor analysis indicates the transformation of the extracted factors (before rotation) to the rotated factors (after applying Varimax rotation) (Weide and Beauducel, 2019). It gives correlation between the original factors and the rotated factors and this assists in explaining the factors in a more understandable way.

Figure 1: Scree plot



Source(s): Authors

Factor 1 of the original factors has a high correlation with rotated Factor 1 (0.728) and a moderate negative correlation with rotated Factor 2 (−0.683), meaning that it is a major contributor to rotated Factor 1, but also is somewhat negatively correlated with rotated Factor 2. Whereas Factor 2 of the original factors is moderately correlated with rotated Factor 1 (0.556) and strongly correlated with rotated Factor 2 (0.643) indicating that it provides a greater contribution to rotated Factor 2.

Factor 3 shows a very weak negative correlation with rotated Factor 1 (−0.065) and moderate negative correlation with rotated Factor 2 (−0.526), indicating that it has a small contribution to rotated Factor 1 and a significant contribution to rotated Factor 2. The data collected about women and youth e-commerce entrepreneurs in Bangladesh were analyzed using the exploratory factor analysis (EFA), which reflected three unique factors that affected their awareness of cybersecurity. Principal Axis Factoring (PAF) with Varimax rotation was used to derive these factors, where a better understanding of the underlying constructs was clear. The findings of each of the factors are given below in detail:

The initial and the most salient one that we designated as Cybersecurity Knowledge and Practices explained the greatest variation in the data. This dimension is mostly related to the knowledge of the respondents on cybersecurity threats, their implementation of protective security measures, and their perception of the danger of cyberattacks. Security Practices 1 (e.g., use of strong passwords) and Risk Perception 1 (e.g., awareness of the severity of cybersecurity threats), had strong loadings on this factor with value of 0.851 and 0.839, respectively. It means that women and the youth e-commerce entrepreneurs who have a better understanding of the dangers associated with cybersecurity are more likely to take necessary precautionary measures. Moreover, those respondents with a perception of the significance of protecting customer information and business functionality through two-factor authentication and routinely backing up their information scored high on this aspect. The high loading of Cybersecurity Knowledge 2 that assesses knowledge about customer data protection further supports the value of cybersecurity knowledge in influencing protective practices.

In this regard, Risk Perception is also important to highlight the critical role of the latter in shaping security behaviors. Respondents who hold that cyber threats are serious and harmful to their business activities stand better chances of taking proactive measures towards addressing the threats. The second variable, Digital Literacy, indicates how well the respondents are able to employ digital platforms safely and efficiently in their businesses. This aspect is highly related to the trust that the entrepreneurs have on their ability to control their privacy settings, online payment systems, and security of their devices and accounts by updating them on a regular basis.

Some of the highest area loadings were Digital Literacy 1 (confidence in using digital platforms) and Digital Literacy 3 (ability to manage online payment systems) with high loadings of 0.769 and 0.762, respectively, meaning that the more digitally literate entrepreneurs are, the better they can implement secure online practices. The correlation between digital literacy and security practices is clear, with the level of entrepreneurship in terms of using their digital tools effectively also being connected to some security practices, such as strong passwords (Security Practices 2 with a loading of 0.779) and two-factor authentication.

This aspect outlines the fact that the higher the digital literacy, the greater the chances of implementing cybersecurity measures, which means that knowledge in handling digital devices and privacy controls are essential to promote cybersecurity awareness. The third factor that we described as Training and Institutional Support, reflects the impact of formal education and institutional resources on improving cybersecurity awareness. This aspect demonstrates the significance of training courses and external assistance in enhancing cybersecurity awareness of the e-commerce entrepreneurs.

The loadings of the variables like Training and Institutional Support 3 (training about cybersecurity threats) and Training and Institutional Support 4 (availability of institutional resources in relation to cybersecurity threats) were quite high, 0.815 and 0.777, respectively. These findings indicate that business owners that undergo formal training or are institutional supported are more likely to have a better appreciation of cybersecurity matters and implement suitable security practices. Nonetheless, the smaller loading of Training and Institutional Support 1 (general awareness of training opportunities) at 0.447 means that, although some entrepreneurs are trained, there might be gaps in the access to cybersecurity training (in general or broadly). This observation highlights the necessity of a stronger institutional backing and formulation of more comprehensive and specific training to e-commerce entrepreneurs.

6. CONCLUSION AND IMPLICATIONS

This paper has investigated the cybersecurity awareness among women and youth e-commerce entrepreneurs in Bangladesh through Exploratory Factor Analysis (EFA). The results indicate that cybersecurity awareness is a multidimensional construct, which is influenced by three major dimensions, including cybersecurity awareness and risk perception, digital literacy and security practices, and cybersecurity knowledge with training and institutional support.

One of them appeared to be the strongest factor and it suggests that risk perception is a central factor in influencing cybersecurity behavior. When the entrepreneurs believe that cyber threats are severe and effective, they will be more inclined to practice the protective strategies that can prevent such threats, e.g. using strong passwords, data backup, and safe transaction (Olubunmi et al., 2024). This is in line with the available literature which indicates that perceived vulnerability has a great impact on precautionary behavior.

The second justification is used to justify the relevance of digital literacy in facilitating safe online behavior. More digitally savvy entrepreneurs are becoming more competent in conducting online transactions in a safe way, and a direct result of enhanced cybersecurity behavior (Loukaka and Rahman, 2017). The third consideration highlights the importance of cybersecurity knowledge and training assistance in raising awareness. Although knowledge is a component of awareness, the results show that formal training and institutional support is not evenly distributed with some training related variables having a relatively low contribution (Adleena Huzaizi et al, 2021). This indicates that despite the awareness of cybersecurity threats, entrepreneurs might have no formalized advice and institutional support to mitigate the threats.

The results are valuable to policy makers, training and development agencies that seek to enhance cybersecurity in e-commerce industry (Praditya et al., 2023). To begin with, the good position of risk perception implies that risk awareness campaigns must be aimed at conveying actual cyber risks and impact. Provision of technical knowledge might not be effective enough; the entrepreneurs must also be aware of the real-world effects of cyber threats, including loss of money and reputation, to encourage behavior change.

Second, the importance of digital literacy suggests that the element of cybersecurity ought to be incorporated into the capacity-building programs in the context of digital skills training. Cybersecurity needs to be integrated into the daily digital behaviors, including how we handle online transactions, customer information, and social media to conduct business. Third, the results indicate that there is a clear demand to have accessible and specific training programs on women and youth entrepreneurs. The comparatively poor performance of training related variables indicates the gaps in availability, accessibility, or effectiveness of existing training programs (Wang, 2021). Thus, simplified, practical, and context-specific training modules should be designed to meet the needs of small e-commerce businesses by the institutions. Also, cooperation with IT service providers and industry stakeholders can aid in availing affordable cybersecurity solutions and advisory services to entrepreneurs, overcoming the resource limitations that SMEs are typically limited to (Kaur and Ramkumar, 2022).

7. FUTURE RESEARCH DIRECTION

Although this research offers valuable exploratory research on cybersecurity awareness among women and young e-commerce entrepreneurs in Bangladesh, there are still a number of opportunities that can be explored in further research. One, since this study used Exploratory Factor Analysis (EFA), subsequent research must use Confirmatory Factor Analysis (CFA) to establish the validity of the factor structure that has been identified (Widaman and Helm, 2023). This would assist in determining the reliability and generalizability of the constructs to other samples and situations.

Second, the current study can be expanded in the future by applying Structural Equation Modeling (SEM) in order to investigate the cause-effect relationships between cybersecurity awareness, digital literacy, risk perception, and security practices. This analysis would give a more insight into how these factors interplay and affect real-life cybersecurity behavior (Gombár et al., 2024).

Third, comparative research might be carried out in various population groups, including male business owners, businesses in the country and in cities, or different age groups, to define whether the patterns of cybersecurity awareness are significantly different among the population groups (Zineddine et al., 2024). Fourth, it is suggested that longitudinal study is necessary to determine the levels of cybersecurity awareness over time, specifically in relation to training interventions, policy or policy changes, or exposure to more digital platforms. This would assist in finding out how effective the awareness programs are in the long run.

Fifth, qualitative methods (e.g., interviews or case studies) could be included in the study in the future to better understand the practical issues, lived experiences, and behavioral obstacles encountered by women and young entrepreneurs in coping with cybersecurity risks. Also, it can be scaled up to explore the potential of institutional and technological support systems, such as government programs, training in the private sector, and digital platforms, to improve the cybersecurity preparedness of small businesses (AL-Dosari and Fetais, 2023). Lastly, the possibility of incorporating new technologies to enhance cybersecurity among e-commerce entrepreneurs, especially in the resource-limited settings such as Bangladesh, can be investigated in the future (Liu et al., 2022).

8. ACKNOWLEDGEMENT

The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through a large-group Research Project under grant number (RGP.2/66/47).”

REFERENCES

Abukeshek, M., Al-Mhiqani, M., Parkinson, S., Khan, S., Bearfield, G. (2026), Cybersecurity in intelligent railway systems: Taxonomy, research trends, challenges, and future directions. Computers and Electrical Engineering, 132, 110994.

Adenekan, O.A., Ezeigweneme, C., Chukwurah, E.G. (2024), Strategies for protecting IT supply chains against cybersecurity threats. International Journal of Management and Entrepreneurship Research, 6(5), 1598-1606.

Adleena Huzaizi, A.H., Ahmad Tajuddin, S.N.A., Bahari, K.A., Manan, K.A., Abd Mubin, N.N. (2021), Cyber-security culture towards digital marketing communications among small and medium-sized (SME) entrepreneurs. Asian Culture and History, 13(2), 20.

Ahammed, T., Asad, M., Sakib, K. (2024), Impact of Fourth Industrial Revolution (4IR) on SMEs and Employment in Bangladesh: Opportunities and Challenges; [arXiv Preprint].

Ahmad Zukarnain, Z., Zazira Hashim, M., Muhammad, N., Ahlami Mansor, F., Nor Hazimah Wan Azib, W., Teknologi Mara Kelantan, U., Ilmu, B., Malaysia, K. (2020), Impact of training on cyber security awareness. Gading Journal of Science and Technology, 3(1), 114-120.

Ainslie, S., Thompson, D., Maynard, S., Ahmad, A. (2023), Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers and Security, 132, 103352.

Alahmari, S., Renaud, K., Omoronyia, I. (2023), Moving beyond cyber security awareness and training to engendering security knowledge sharing. Information Systems and E Business Management, 21(1), 123-158.

Alam, S.S., Ahsan, N., Kokash, H.A., Alam, S., Ahmed, S. (2025), A students' behaviors in information security: Extension of protection motivation theory (PMT). Information Security Journal a Global Perspective, 34(3), 191-213.

AL-Dosari, K., Fetais, N. (2023), Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach. Electronics (Switzerland), 12(17), 3629.

Arsenovych, L., Nikolaievsky, O., Skliarenko, O., Lytvynenko, L., Kydriavskyi, I. (2024), Organization of training with the use of digital technologies for ensuring cybersecurity in the educational space. WSEAS Transactions on Computer Research, 12, 524-536.

Ashley, C.J., Preiksaitis, M. (2022), Strategic cybersecurity risk management practices for information in small and medium enterprises. BMRA, 1(2), 109-157.

Aslam, M.A., Li, Z., Shabbir, M.S., Păunescu, L.M., Jaradat, M., Nazir, H., Sinisi, C.I. (2026), Synergistic effects of supplier resilience, information sharing, inventory management, and flexibility on supply chain resilience: A PLS-SEM and NCA approach. Humanities and Social Sciences Communications, 14, 44.

Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., Hossain, M. A. (2025), Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Annals of Operations Research, 350(2), 673-698

Badghish, S., Soomro, Y.A. (2024), Artificial Intelligence adoption by SMEs to achieve sustainable business performance: Application of Technology-Organization-Environment Framework. Sustainability, 16(5), 1864.

Becker, W., Schmid, O. (2020), The right digital strategy for your business: An empirical analysis of the design and implementation of digital strategies in SMEs and LSEs. Business Research, 13(3), 985-1005.

Boopathi, K., Sreejith, S., Bithin, A. (2015), Learning cyber security through gamification. Indian Journal of Science and Technology, 8(7), 642-649.

Chidukwani, A., Zander, S., Koutsakis, P. (2022), A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. IEEE Access, 10, 85701-85719.

Chowdhury, S., Rahman, M., Doddanavar, I.A., Zayed N.M., Nitsenko, V., Melnykovych, O. Holik, O. (2023), Impact of social media on knowledge of the COVID-19 pandemic on Bangladeshi university students. Computation, 11(2), 38.

Corradini, I., Nardelli, E. (2020), Developing digital awareness at school: a fundamental step for cybersecurity education. In: Corradini, I., Nardelli, E., Ahram, T. (eds) Advances in Human Factors in Cybersecurity. AHFE 2020. Advances in Intelligent Systems and Computing, 1219, 1-10.

De Winter, J.C.F., Dodou, D. (2012), Factor recovery by principal axis factoring and maximum likelihood factor analysis as a function of factor pattern and sample size. Journal of Applied Statistics, 39(4), 695-710.

Debb, S.M., Mcclellan, M.K. (2021), Perceived vulnerability as a determinant of increased risk for cybersecurity risk behavior. Cyberpsychology Behavior and Social Networking, 24(9), 605-611.

de Nobrega, K. M., Rutkowski, A.-F., Saunders, C. (2024), The whole of cyber defense: Syncing practice and theory. The Journal of Strategic Information Systems, 33(4), 101861

Elhusseiny, H.M., Crispim, J. (2021), SMEs, barriers and opportunities on adopting Industry 4.0: A review. Procedia Computer Science, 187, 105-111.

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., Pickering, J.B. (2023), Cybersecurity Awareness and Capacities of SMEs. In: International Conference on Information Systems Security and Privacy. p296-304.

Estrada, F. J. R., George-Reyes, C. E., Glasserman-Morales, L. D. (2022), Security as an emerging dimension of Digital Literacy for education: a systematic literature review. Journal of E-Learning and Knowledge Society, 18(2), 22-33.

Gazi, A.I., Mim, A.T., Masud, A.A., Rahman, K.H., Amin, M.B., Senathirajah, A.R., Bin S., Oláh, J. (2025), Paving the way of entrepreneurship for university students: The role of innovativeness, technological adaptability, and self-management, with risk-taking and family support as moderator. Cogent Education, 12(1), 2455230.

Germanos, G., Lekidis, A., Brotsis, S., Kolokotronis, N. (2026), Blockchain architectures for enhancing EV infrastructure security: A unified framework for addressing sophisticated cyber-attacks. Future Generation Computer Systems, 182, 108426.

Ghobakhloo, M., Iranmanesh, M., Vilkas, M., Grybauskas, A., Amran, A. (2022), Drivers and barriers of Industry 4.0 technology adoption among manufacturing SMEs: A systematic review and transformation roadmap. Journal of Manufacturing Technology Management, 33(6), 1029-1058.

Gold, K.L. (2025), Effects of industry 4.0 on small and medium-scale enterprises: An analytical and bibliometric review. SAGE Open, 15(2), 1-18.

Gombár, M., Vagaská, A., Korauš, A., Račková, P. (2024), Application of structural equation modelling to cybersecurity risk analysis in the Era of industry 4.0. Mathematics, 12(2), 343.

Goretzko, D., Pham, T.T.H., Bühner, M. (2021), Exploratory factor analysis: Current use, methodological developments and recommendations for good practice. Current Psychology, 40(7), 3510-3521.

Haq, I.U., Huo, C. (2023), Digital strategy and environmental performance: The mediating role of digitalization in SMEs. Digital Economy and Sustainable Development, 1(1), 9.

Haque, R., Senathirajah, A.R.B.S., Khalil, M.I., Qazi, S.Z., Ahmed, S. (2024), A structural path analysis Bangladeshi SMEs' sustainability through social media marketing. Sustainability (Switzerland), 16(13), 5433.

Hirvonen, J., Majuri, M. (2020), Digital capabilities in manufacturing SMEs. Procedia Manufacturing, 51, 1283-1289.

Hossain, M.B., Rahman, M.U., Čater, T., Vasa, L. (2025), Determinants of SMEs' strategic entrepreneurial innovative digitalization: Examining the mediation role of human capital. European Journal of Innovation Management, 28(7), 2733-2760.

Hossain, S., Hassan, S., Karim, R. (2023), Assessment of critical barriers to Industry 4.0 adoption in manufacturing industries of Bangladesh: An ISM-based study. Brazilian Journal of Operations Production Management, 20(3), 1797.

Iqbal, M.M., Islam, K.M.A., Zayed, N.M., Beg, T.H., Shahi, S.K. (2021), Impact of artificial intelligence and digital economy on industrial revolution 4: Evidence from Bangladesh. American Finance and Banking Review, 6(1), 42-55.

Isa, R.A., Setiawan, B., Pakaja, F. (2026), Cybersecurity awareness in the digital commerce ecosystem: Factor analysis, program impact and

future trends for consumers and MSMEs. Information and Computer Security, 1-26.

Islam, M.A., Mian, E.A., Ali, M.H. (2009), Factors affecting business success of Small and medium enterprises (SMEs) in Bangladesh. Business Review, 4(2), 123-138.

Islam, N., Bhuiyan, F., Karim, S. (2025), Sustainability practices in SMEs: An explorative study on ethnic minority-owned SMEs in the United Kingdom. Business Strategy and the Environment, 35, 4189-4209.

Kabir, S., Reem, M.T. (2025), Impact of the fourth industrial revolution on society: A global perspective. Asian Journal of Agricultural Extension Economics and Sociology, 43(6), 150-158.

Kanbacha, R., Kraus, S., Jones, P. (2024), The new normal: The status quo of AI adoption in SMEs. Employee Relations, 46(3), 2379999.

Kaur, J., Ramkumar, K.R. (2022), The recent trends in cyber security: A review. Journal of King Saud University Computer and Information Sciences, 34(8), 5766-5781.

Khan, N., Furnell, S., Bada, M., Rand, M., Nurse, J.R.C. (2025), Investigating the experiences of providing cyber security support to small- and medium-sized enterprises. Computers and Security, 154, 104448.

Khayer, A., Jahan, N., Hossain, M.N., Hossain, M.Y. (2021), The adoption of cloud computing in small and medium enterprises: A developing country perspective. VINE Journal of Information and Knowledge Management Systems, 51(1), 64-91.

Kostyuk, N., Wayne, C. (2021), The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. Journal of Global Security Studies, 6(2), 077.

Ledesma, R.D., Valero-Mora, P., Macbeth, G. (2015), The scree test and the number of factors: A dynamic graphics approach. The Spanish Journal of Psychology, 18, E11.

Liu, X., Ahmad, S.F., Anser, M.K., Ke, J., Irshad, M., Ul-Haq, J., Abbas, S. (2022), Cyber security threats: A never-ending challenge for e-commerce. Frontiers in Psychology, 13, 927398.

Loukaka, A., Rahman, S.S.M. (2017), Discovering new cyber protection approaches from a security professional prospective. International Journal of Computer Networks and Communications, 9(4), 13-25.

Mazumdar, A., Alharahsheh, H. (2019), Small & medium enterprises (SMES) - insights of Bangladeshi SMES in different contexts of adopting cloud computing. Cross Current International Journal of Economics Management and Media Studies, 1(5), 130-140.

McCrohan, K.F., Engel, K., Harvey, J.W. (2010), Influence of awareness and training on cyber security. Journal of Internet Commerce, 9(1), 23-41.

Menard, P., Bott, G.J., Crossler, R.E. (2017), User motivations in protecting information security: Protection motivation theory versus self-determination theory. Journal of Management Information Systems, 34(4), 1203-1230.

Mia, M.M., Rizwan, S., Zayed, N.M., Nitsenko, V., Miroshnyk, O., Kryshtal, H., Ostapenko, R. (2022), The impact of green entrepreneurship on social change and factors influencing AMO theory. Systems, 10(5), 132.

Mogaji, E., Oke, A., Adewale, A. (2024), Determinants of digital technology adoption in innovative SMEs. Journal of Innovation Knowledge, 9(4), 100610.

Nawaz, S., Makin, F., Bashir, T., Habib, Q., Shabbir, M.S., Aslam, E. (2025), Cultural norms and safety management: Understanding honour killing in Pakistan. Journal of Asian Development Studies, 14(2), 958-970.

Ng, P.S.J., Zhang, X., Fu, L., Ye, L., Phan, K.Y. (2025), The inclusive innovation of blockchain in securities issuance: Reduced inequalities of investors. Journal of Advanced Research in Applied Sciences and Engineering Technology, 46(2), 188-212.

Nishu, M.A., Tat, H.H., Kumarusamy, R., Hafiz, N., Karim, I.U., Fazal, S.A., Hasnat, A. (2025), Entrepreneurial marketing and SME performance: The mediating role of process and product innovation in Bangladesh. Journal of Posthumanism, 5(5), 2163-2186.

Ntlatlapa, N. (2023), Defining the fourth industrial revolution. South African Journal of Science 119(1-2), 12916.

Oakley Browne, T., Pardede, E. (2026), A systematic review on adversarial thinking in cyber security education: Themes and potential frameworks. Computers and Security, 163, 104803.

Pandya, V.M. (2012), Comparative Analysis of Development of SMEs in Developed and Developing Countries. In: The 2012 International Conference on Business and Management 6 - 7 September 2012, Phuket - Thailand.

Panko, M., Šafár, L., Meštan, M. (2025), Small firms, big threats: Cybersecurity research and the role of public policy in the SME sector. Central European Journal of Public Policy, 19(2), 87-110.

Patterson, C.M., Nurse, J.R.C., Franqueira, V.N.L. (2024), "I don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents. Computers and Security, 139, 103699.

Pavlova, O.Y., Panchenko, V.I., Rohozha, M.M., Stoian, S.P., Turenko, V.E., Zayed, N.M. (2021), An entrepreneurial transformation and organization of quarantine cultural practices in the smart city: Evidence from Ukraine. Academy of Entrepreneurship Journal, 27(6), 1-6.

Prada, M.A., Fuertes, J.J., Rodríguez-Ossorio, J.R., González-Herbón, R., González-Mateos, G., Domínguez, M. (2023), Hands-on training in industrial cybersecurity for a multidisciplinary Master's degree. IFAC-PapersOnLine, 56(2), 11217-11222.

Praditya, E., Maarif, S., Ali, Y., Saragih, H.J.R., Duarte, R., Suprapto, F.A., Nugroho, R. (2023), National cybersecurity policy analysis for effective decision-making in the age of artificial intelligence. Journal of Human Security, 19(2), 91-106.

Prasanna, R.P.I.R., Jayasundara, J.M.S.B., Gamage, S.K.N., Ekanayake, E.M.S., Rajapakshe, P.S.K., Abeyrathne, G.A.K.N.J. (2019), Sustainability of SMEs in the competition: A systemic review on technological challenges and SME performance. Journal of Open Innovation Technology Market and Complexity, 5(4), 100.

Rahman, H., Majumder, S.C. (2020), Feasibility of NGO Initiatives in SME, rural benefits and challenges: A case study in Cumilla, Bangladesh. Journal of Economic Info, 7(1), 26-39.

Rehman, A.U., Malik, A.H., Shabbir, M.S., Hussain, A., Raza, K.M. (2023), Does sharia tag constitute heuristic while choosing an Islamic financial institute? Evidence from Pakistan. GISRAS Journal of Management Islamic Finance (GJMIF), 3(4), 1.

Ruohonen, J., Rindell, K., Busetti, S. (2025), From cyber security incident management to cyber security crisis management in the European Union. Computers and Security, 159, 104689.

Rupa, R.A., Meher, F., Tarek, S., Saif, A.M., Arefin, S., Mostafa, R. (2026), IoT adoption for sustainable performance in SMEs using an SEM-ANN approach. Discover Internet of Things, 6, 20.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., Cano, J.J.M. (2019), An effective cybersecurity training model to support an organizational awareness program: The cybersecurity awareness training model (CATRAM), A case study in Canada. Journal of Cases on Information Technology, 21(3), 26-39.

Sagita, A., Yusof, M.S.M., Budiharjo, R., Nsereko, I., Suhimi, S. (2025), Entrepreneurial networking as a mediator between entrepreneurial orientation and business performance: Insights from small business owners in Malaysia. Asian Economic and Financial Review, 15(1), 76-97.

Santos, A.M., Sant'Anna, Â.M.O. (2024), Industry 4.0 technologies for sustainability within small and medium enterprises: A systematic

literature review and future directions. Journal of Cleaner Production, 467, 143023.

Sas, M., Reniers, G., Ponnet, K., Hardyns, W. (2021), The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour. Safety Science, 144, 105447.

Shahadat, M.M.H., et al. (2023), Digital technology adoption in SMEs: TOE framework analysis. International Journal of Management Studies, 11(2), 110-120.

Shahzad, A., Zakaria, M.S.A., Kotzab, H., Makki, M.A.M., Hussain, A., Fischer, J. (2023), Adoption of fourth industrial revolution 4.0 among Malaysian small and medium enterprises (SMEs). Humanities and Social Sciences Communications, 10(1), 693.

Suhail, S., Iqbal, M., McLaughlin, K., Lee, B., Imtiaz, B. (2025), A framework for enhancing cyber incident response with security-enhancing digital twins in cyber-physical systems. Internet of Things, 31, 101547.

Tavakol, M., Dennick, R. (2011), Making sense of Cronbach's alpha. International Journal of Medical Education, 2, 53-55.

Techanamurthy, U., Iqbal, M.S., Rahim, Z.A. (2025), Industry 4.0 readiness and strategic plan failures in SMEs: A comprehensive analysis. PLoS One, 20(5), e0324052.

Thakur, OA., Alam, M.K. (2022), The Problems and Challenges of Small and Medium Enterprises in Bangladesh. Available from: https://www.isu.ac.bd/journal

Tobias, S., Carlson, J.E. (1969), Brief report: Bartlett's test of sphericity and chance findings in factor analysis. Multivariate Behavioral Research, 4(3), 375-377.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., Kusev, P. (2017), Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior, 75, 547-559.

Veksler, V.D., Buchler, N., Hoffman, B.E., Cassenti, D.N., Sample, C., Sugrim, S. (2018), Simulations in cyber-security: A review of cognitive modeling of network attackers, defenders, and users. Frontiers in Psychology, 9, 691.

Vladimirovna, N.E. Zayed, N.M. (2021), Digital industrialization: Entrepreneurial features of advanced nations' innovation policies during industrial revolution 4.0. Academy of Entrepreneurship Journal, 27(6), 1-8.

Wang, S. (2021), Study on the application of computer security technology in e-commerce. Journal of Physics Conference Series, 1915(4), 042044.

Weide, A.C., Beauducel, A. (2019), Varimax rotation based on gradient projection is a feasible alternative to SPSS. Frontiers in Psychology, 10, 00645.

Widaman, K.F., Helm, J.L. (2023), Exploratory factor analysis and confirmatory factor analysis. In: Cooper, H., Coutanche, M.N., McMullen, L.M., Panter, A.T., Rindskopf, D., Sher, K.J., editors. APA Handbook of Research Methods in Psychology: Data Analysis and Research Publication. 2nd ed. United States: American Psychological Association. pp. 379-410.

Yuwono, T., Suroso, A., Novandari, W. (2024), Information and communication technology in SMEs: A systematic literature review. Journal of Innovation and Entrepreneurship, 13, 31.

Zineddine, A., Chakir, O., Sadqi, Y., Maleh, Y., Singh Gaba, G., Gurtov, A., Dev, K. (2024), A systematic review of cybersecurity assessment methods for HTTPS. Computers and Electrical Engineering, 115, 109137.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., Basim, H. N. (2022), Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97