APAC Cybersecurity Fund
The Asia Foundation

VWEC

REPORT

FEMALE-OWNED AND LED BUSINESSES:

THE NEED FOR INFORMATION SECURITY TRAINING IN DIGITAL ECONOMY

HANOI, JULY 2024

CyberPeace Institute
GLOBAL CYBER ALLIANCE

with support from Google.org

REPORT

FEMALE-OWNED AND LED BUSINESSES:

THE NEED FOR INFORMATION SECURITY TRAINING IN DIGITAL ECONOMY

Hanoi, July 2024

Acknowledgements

We would like to express our gratitude to the Viet Nam Women Entrepreneurs Council (VWEC) at the Viet Nam Chamber of Commerce and Industry (VCCI) and The Asia Foundation in Viet Nam (TAF) for their invaluable cooperation in preparing this report, titled "Female-Owned and Led Businesses: The Need for Information Security Training in Digital Economy".

The report was prepared by a group of consultants, to compile information and data on businesses owned and led by women. It highlighted the need for information security training within the digital economy and its contribution to implementing the *"Supporting the development of businesses owned and led by women in Viet Nam"* Project between 2024 and 2027.

We would also like to thank all the partners, associations, companies, and individuals who kindly provided important information during our research. Specifically, our colleagues at TAF, including Mrs. Nguyen Thi Ngoc Anh and Mrs. Tran Giang Linh, as well as experts from the Information Technology Institute (ITI) of Viet Nam National University, Hanoi.

Particularly, immense efforts have been made to ensure the accuracy and objectivity of the information and data presented. However, it is not possible to guarantee that all of the information is completely accurate or updated due to the limitations of the info collecting form, the time it took to collect information, the information security incidents, and the ongoing technological change. Therefore, our team of consultants look forward to receiving your feedback.

Disclaimer: The comments and assessments in this report are those of the consultant team and do not necessarily reflect the views of the VWEC, the VCCI, the TAF or any individuals and organizations mentioned.

Table of contents

List of figures

Introduction

With digital platforms and tools being the primary force behind the sustainability and growth of Viet Nam's micro, small, and medium-sized enterprises (MSME), it is undeniable that the digitalization of Vietnamese businesses is becoming more prevalent than ever, particularly after the COVID-19 pandemic. However, these businesses now must deal with a new challenge: Information Security.

According to a report by Kaspersky, in the first quarter of 2024, there were 5% more malware attacks in small and medium-sized enterprises than the same period the previous year[1]. Viet Nam was recorded as the third most vulnerable Southeast Asian country in 2022 in terms of cyber security threats (behind only Indonesia and Thailand). Compared to the same period in 2023, there were 70% more ransomware assault operations in Viet Nam during the first quarter of 2024 that encrypted the data and virtualization infrastructure of businesses and organizations[2]. It calls for prompt action to be taken to bridge the knowledge and practice gaps that exist between the dangerous digital landscape and Vietnamese enterprises, particularly those owned and led by women, to enhance their capacity to grow in the digital economy and adapt safely in cyberspace.

The Viet Nam Women Entrepreneurs Council (VWEC) at the Viet Nam Chamber of Commerce and Industry (VCCI) and The Asia Foundation in Viet Nam (TAF) implements the **"Supporting the development of Female-Owned and Led Businesses in Viet Nam"** Project from 2024 to 2027. The Project aims to support the growth and development of businesses of micro, small and medium enterprises owned and led by women, which is through capacity building to effectively use digital platforms and tools to become more competitive in the digital economy.

In June 2024, the consulting team of VWEC carried out a survey to determine the information security training requirements of female-owned and led businesses. The collected data will serve as the foundation for crafting more suitable and successful company capacity building initiatives on digital information security. Furthermore, the VWEC can also utilize these data to map out future activities and development programs for its members.

1 https://thanhnien.vn/kaspersky-tinh-trang-tan-cong-mang-doanh-nghiep-vua-va-nho-gia-tang-185240628150022042.htm

2 Báo cáo "Tình hình nguy cơ mất ATTT tại Việt Nam quý 1/2024", Viettel Threat Intelligence

The process of gathering information and data about the target beneficiary group and assessing training needs is the first step in the training process. It helps to affirm that training is the most effective solution to enabling female entrepreneurs and female-owned and led businesses to improve their business performance. Assessing training needs involves evaluating and analyzing the gap between current knowledge and practices to identify deficiencies in knowledge and skills among female entrepreneurs and their businesses.

Main contents

I. General Information

1. Objectives

1.1. General Objectives

The report aims to compile information and data about multiple Vietnamese business groups owned and led by women and assess their training needs to contribute to the effective implementation of the "Supporting the Development of Female-Owned and Led Businesses in Viet Nam" Project. This includes enhancing awareness of information security in the digital economy for businesses owned and led by women. The project is carried out by the Viet Nam Women Entrepreneurs Council at the Viet Nam Chamber of Commerce and Industry (VCCI) in collaboration with The Asia Foundation in Viet Nam, from 2024 to 2027.

To achieve the abovementioned objective, the consulting team had conducted research, selected examples, and distributed questionnaires, then conducted in-depth interviews with women's business associations, clubs, and members within the Viet Nam Women Entrepreneurs Council's network (VWEC for short). The goal was to understand and assess their awareness, current situation, and training needs regarding information security in the digital economy. Then, the information was used to identify groups that need training and develop a report assessing their needs for information security training.

In the end, the report will also serve as a foundation for the VWEC and TAF to develop materials and design training programs tailored to the needs and actual context of information security for female-owned and led businesses in Viet Nam.

1.2. Specific Objectives

- Compile information and data about beneficiary groups, which are women-owned and led businesses from VWEC and VCCI's network, particularly about business sizes, business fields, development stages, and demographic information about the business owners.
- Learn about the level of information security-related knowledge that female entrepreneurs have.
- Explore key aspects of information security implementation within a business.
- Identify the training needs of businesses in terms of information security: topics, duration, formats…
- Propose a training program that aligns with the needs of women-owned and led businesses.

2. Scope and Target Groups

- Scope of the Study: The information security training needs of women-owned and led businesses, focusing on course content, formats, and duration.
- Target Groups for Feedback and Needs Assessment:
    - Women-owned and led businesses in Viet Nam.
    - Women entrepreneurs' associations, clubs, and organizations (hereafter referred to as "Association Organizations") within the network of the VWEC.

3. Research methods

To gather information and data about the beneficiary group and assess training needs for information security through stakeholders, the report employs a combination of quantitative and qualitative methods.

3.1. Quantitative Research

Focusing on descriptive statistical analysis of the beneficiary group, their awareness of information security, the current state of information security practices within businesses, and their training needs. The information will be used to propose content and methods for information security training in the digital economy for women-owned and led businesses. Data collection was conducted via an online Google Forms survey. The questions were designed with single-choice, multiple-choice, or open-ended formats, including 13 questions for the association organizations and 18 questions for women-owned and led businesses.

3.2. Qualitative Research

Reviewing secondary documents and conducting in-depth interviews. Results from the quantitative research and secondary documents were combined with findings from the interviews to provide comprehensive insights. The qualitative research was carried out concurrently with the quantitative research, involving in-depth interviews with six participants from women's business associations and women-owned and led businesses in Hanoi, Hai Duong, and Hung Yen. The interview questions were like those in the quantitative survey but included more detailed questions specific to each business/association. During the interviews, open-ended questions were used to clarify arising issues.

Limitations of the abovementioned research methods:

- The in-depth interviews were only conducted in the northern region.
- The quantitative research method may not fully capture the subjective factors and personal experiences of the businesses.
- The quantitative survey sample was randomly selected nationwide; however, the response rate was higher in the northern region. This may be due to the larger and more frequently

engaged network of associations and women entrepreneurs affiliated with the Viet Nam Women Entrepreneurs Council in the North.

- The short timeframe for collecting feedback meant that the survey design was not very detailed and just focused on quickly assessing the awareness and training needs of women-owned and led businesses.

II. General Information about Association Organizations and Businesses Owned and Led by Women

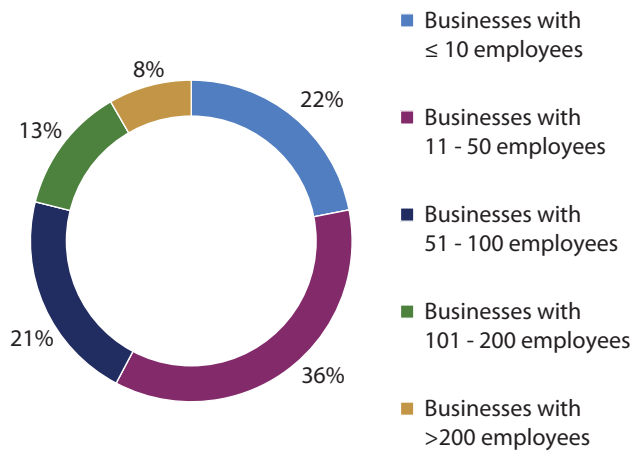
1. Information about Association Organizations

The consulting team sent questionnaires to 34 VWEC Association Organizations nationwide and only 21 of them answered (62%), while others chose not to respond due to a lack of interest or not having enough member data required by the questionnaires. Therefore, the number of response papers the consulting team gathered is 21 (one per province/city). Among these, the response rate from Association Organizations in the Northern region has the largest percentage with 57.14%, followed by the Central region at 23.81%, and the Southern region with the lowest percentage of 19.05%.

Furthermore, the 21 Association Organizations have a total of 3,262 members. The organization with the fewest members is the Women Entrepreneurs Club of Ca Mau Province (25 members) while the organization with the most members is the Women Entrepreneurs Association of Thai Nguyen Province (360 members). Most respondents were leaders (President, Vice President of the association), making up 62%, while the remaining 38% are from department heads and above.

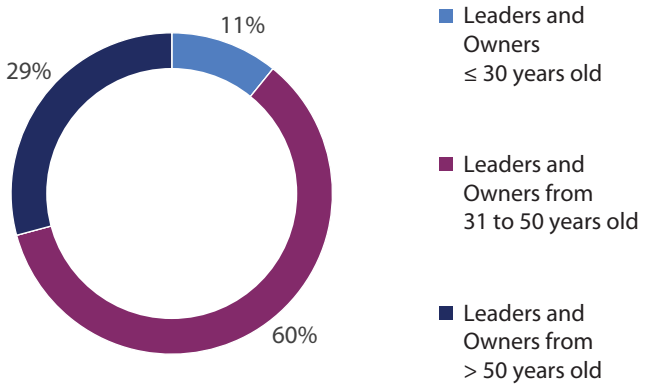
Regarding the size of the members, businesses with 10-50 employees make up the largest proportion (36%), while those with over 200 employees make up the smallest proportion (8%). This may indicate that more smaller businesses participate in the VWEC than larger businesses, possibly given a greater need for networking, learning experiences, seeking business partners, or collectively voicing concerns to regulatory authorities. (see Figure 1).

FIGURE 1: **Businesses' sizes (by number of employees)**



Regarding the age of membership business owners, the majority are between the ages of 31 and 50, making up 60% of the total number of members, which indicates that most business owners are in the middle age range (as they have likely accumulated experience and are advancing in their careers). The over-50 age group accounts for 29%, which is nearly one-third of the total. Younger owners and leaders under 30 years old constitute the smallest proportion at 11%. (see Figure 2).

FIGURE 2. **Age range of members**

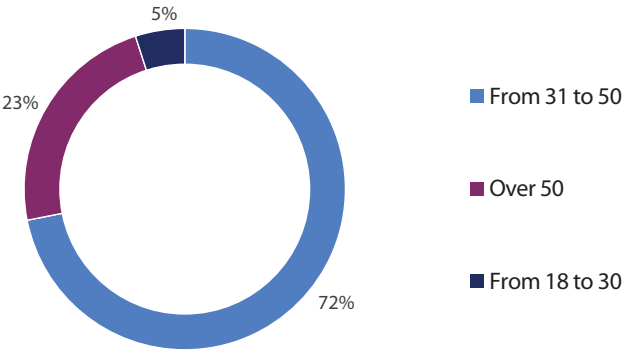


2. Information about Businesses Owned and Led by Women

The consulting team received a total of 122 responses from businesses owned and led by women across 29 provinces and cities nationwide. These responses were collected by sending questionnaires to 34 association organizations, who then forwarded them to the businesses for filling in the form. Additionally, the consulting team sent questionnaires directly to 100 women-led businesses within the network of the Viet Nam Women Entrepreneurs Council across the country. The response rate from women-led businesses in the Northern region was the highest at 57.37%, while the Central region accounted for 15.57%, and the Southern region made up 27.06%. Many businesses and association members did not respond due to either being busy, a lack of interest, or hesitation about completing survey forms.

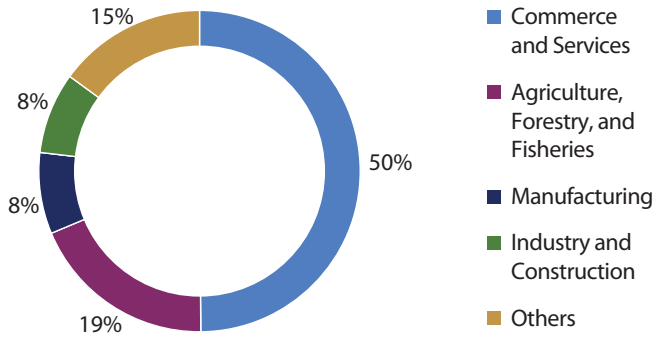
Regarding the age of female business owners, the 31-50 age group represents the largest proportion (72%) among the respondents. The over-50 age group accounts for a lower percentage (23%) but still constitutes a significant proportion, while the 18-30 age group makes up the smallest percentage with only 5% (see Figure 3).

FIGURE 3: **Age range of female business owners**



Regarding the specific fields of the 122 surveyed businesses, 50% are engaged in commerce and services; 19% are involved in agriculture, forestry, and fisheries; 8% operate in industry and construction; and 8% are manufacturers (see Figure 4).

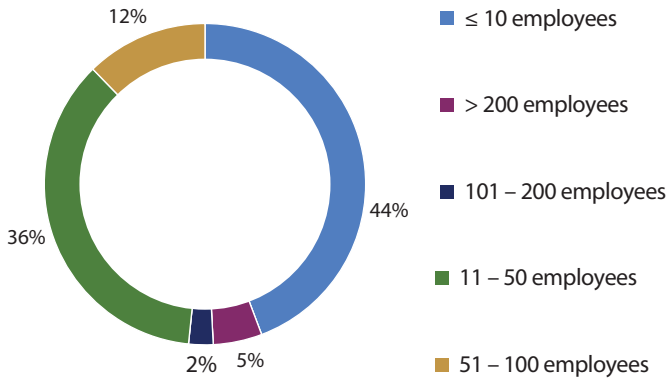
FIGURE 4: **Specific fields of women-owned and led businesses**



Regarding the size of businesses, the group of businesses with 1 to 10 employees represents the largest proportion at 44%. This is followed by the group with 11 to 50 employees, which accounts for 36%; these businesses are of a medium size, capable of expanding operations while maintaining flexibility. Businesses with 51 to 100 employees and those with more than 200 employees represent 12% and 5%, respectively. The group with 101 to 200 employees has the smallest proportion at 2%.

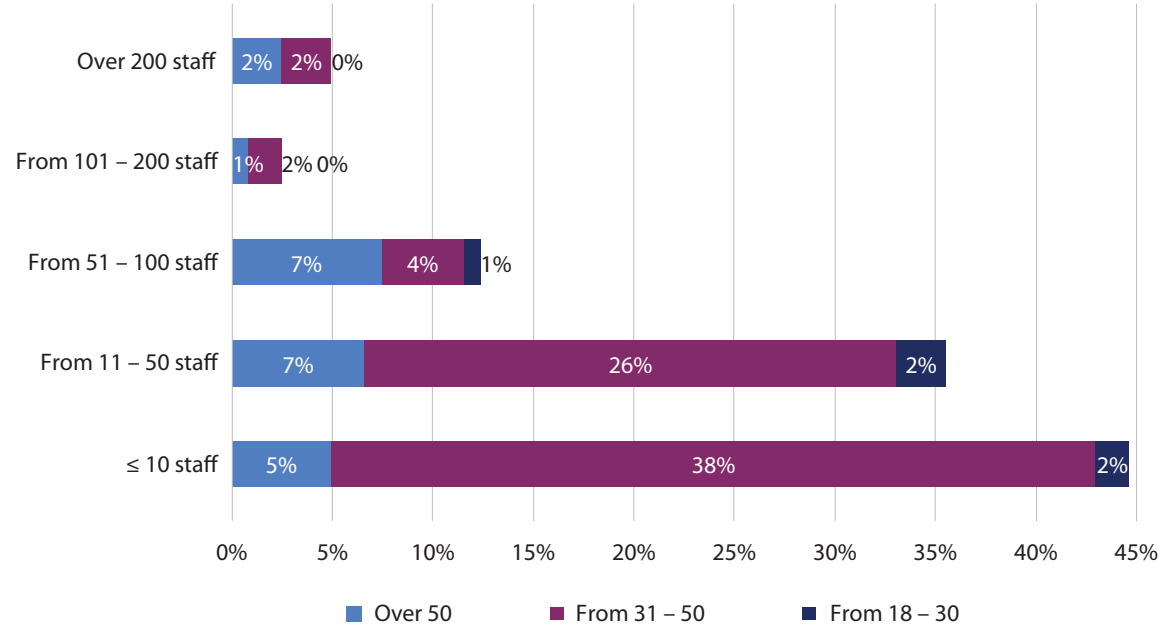
The chart below also shows that the majority of women-owned and led businesses are small and medium-sized, with most employing between 1 and 50 people. This reflects a structural characteristic of Vietnamese businesses in the economy where micro and small businesses predominate (see Figure 5).

FIGURE 5: **Number of employees in women-led and owned businesses**



Notably, owners of businesses employing 100 or more people are not in the age group of 18-30. For businesses with fewer than 10 employees, owners aged 31-50 represent the largest proportion (38%). Even among businesses with 10-50 employees, the proportion of owners aged 31-50 is significantly higher compared to other age groups (26%). As such, this indicates that the age range of 31-50 is ideal for running a business, which can be explained that women in this age group typically have accumulated substantial experience, financial stability, management skills, and a broad network of relationships—factors that contribute to successfully managing a business (see Figure 6).

FIGURE 6: **Age range of business owners and sizes of businesses**



III. Assessing Information Security Training Needs of Women-Owned and Led Businesses

1. Assessing the Current State of Information Security and Awareness

Based on several reports, studies, and practical experiences, common information security incidents faced by Vietnamese businesses can be categorized into five groups: external threats, third parties, customers, internal infrastructure, and internal personnel. Specifically:

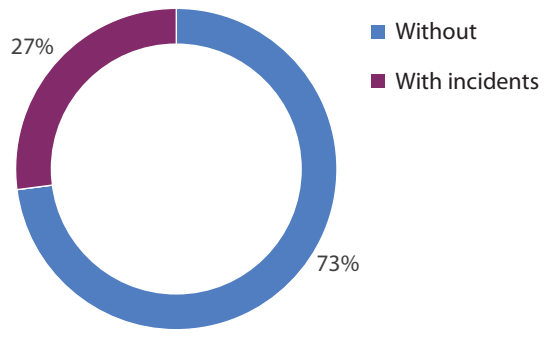
- Information security incidents caused by external threats such as cybercriminals, terrorist groups, and hackers. These groups typically engage in activities such as:
    - Hijacking business email accounts to impersonate the company and request customers to transfer order deposits.
    - Using phishing emails to trick victims into clicking on malicious links or downloading harmful software.
    - Stealing data.
    - Breaching into businesses' systems.
- Information security incidents caused by third parties: These incidents are triggered by service providers working with the business, such as cloud technology providers,

document and data storage services, or essential systems. It can also include partners or contractors who are granted excessive access to perform tasks within the scope of their collaboration, leading to the exposure of confidential or sensitive business data. For instance, an advertising company or a media representative hired to post content on online channels (such as the business's website, Facebook page, TikTok, LinkedIn, YouTube, etc.) might be granted higher access than necessary, increasing the risk of losing accounts or compromising customer data.

- Information security incidents caused by customers: These occur when customers accidentally share their personal information or data with the wrong person or fall victim to malicious software.
- Information security incidents related to infrastructure security: They include incidents involving computers and end-user devices, network systems, and cloud resources (both hardware and software). Infrastructure security involves not only protection from traditional cyberattacks but also protection from natural disasters (floods) and human errors (fires or explosions).
- Information security incidents caused by internal staff: This is a common threat that arises from mistakes, a lack of knowledge, or poor awareness of cybersecurity among staff. Examples include losing devices, using weak passwords, unintentionally disclosing sensitive information, failing to secure data, or becoming the target of a cyberattack. Additionally, internal personnel may deliberately misuse legitimate credentials to steal information for profit, modify or delete critical and confidential data, or install malware to disrupt system operations.

According to the collected data, a significant number of female-owned and led businesses have experienced information security incidents: 27% of businesses reported having encountered such incidents, while 73% stated they had not faced any. (see Figure 7).

FIGURE 7: **Number of businesses encountering information security incidents**



Among the four businesses that underwent in-depth interview (located in Hanoi, Hai Duong and Hung Yen), one business had experienced an information security breach that resulted in financial losses. Specifically, this business had its email account hacked, fraudsters stole transaction information regarding orders with foreign customers, leading to financial damage. Additionally, the company's accounting department's computer was infected with a virus, disrupting their work.

A building materials manufacturer in Northern Viet Nam had experienced the following information security incident:

The email account of an employee in the export department was hijacked by a fraudster who used this email address to communicate with an Australian customer and requested a 50% deposit for an upcoming order. Trusting the authenticity of the email, the Australian customer transferred the requested advance payment.

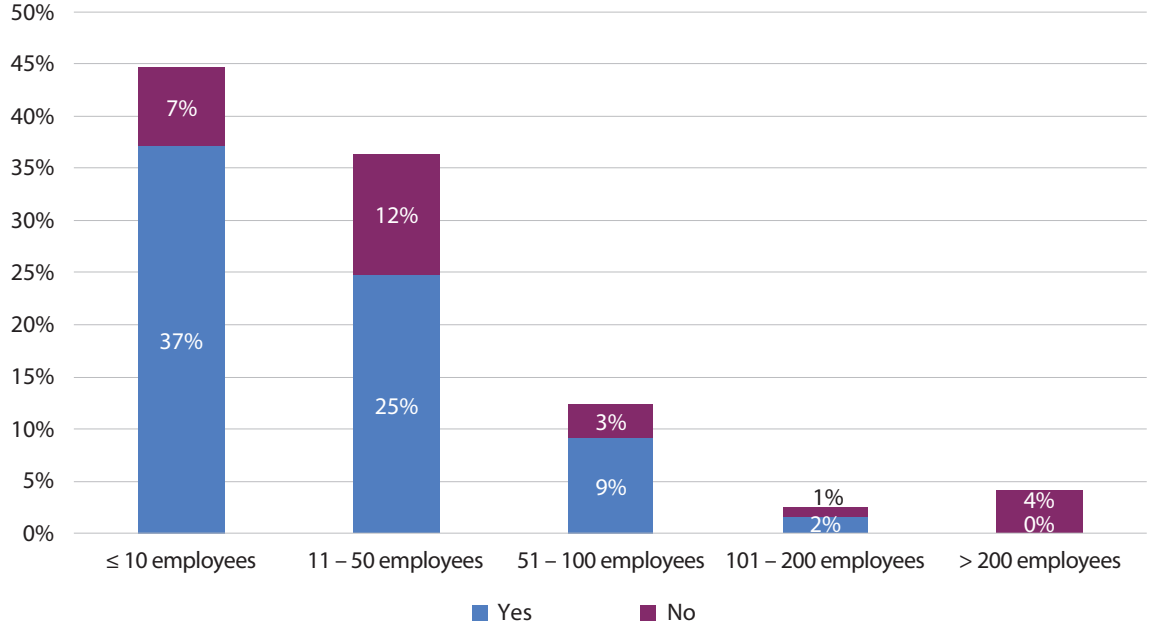
However, when the expected delivery date passed without receiving the goods, the customer contacted the company to inquire. It was only then that the company realized that the export department employee's email had been usurped and misused.

To protect its reputation and maintain the business relationship with the customer, the company decided to fulfill the order as initially agreed. This resulted in a loss of 50% of their order value since the deposit had been stolen by the fraudster. Following the incident, which was a costly lesson about the importance of information security in international business, the company took swift actions, such as replacing their email system with a more secure one and providing information security training to employees to prevent similar occurrences.

(Source: A business that participated in the in-depth interview)

All large-scale businesses reported they had encountered information security incidents. This reflects the ongoing issue of hackers targeting large businesses for attacks. Once the size of a business increases, the likelihood of encountering information security risks also rises. (see Figure 8).

FIGURE 8: **Correlation between business sizes and information security incidents**

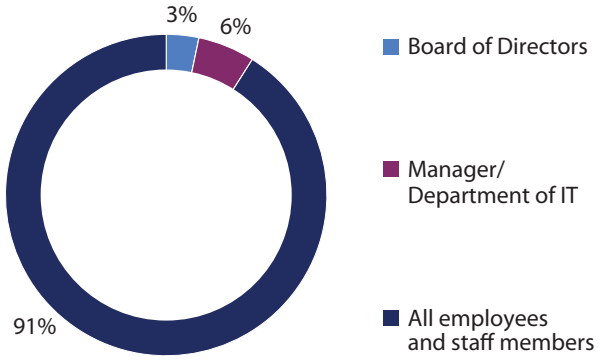


Most businesses correctly understand that ensuring information security is the responsibility of all employees.

Information security is protected when all employees, customers, partners, and third parties are aware of the potential risks and issues related to information security, along with their respective responsibilities and legal obligations. It is essential for them to be equipped with the requisite knowledge and conditions to support the company's information security policies and mitigate risks attributable to human error.

In fact, a substantial 91% of businesses correctly perceive that the responsibility for protecting information security is a collective duty of all employees. This perception has been underpinned by information security and cybersecurity training courses and seminars conducted by the Viet Nam Women Entrepreneurs Council, the Department of Information and Communications, the Provincial Women's Union, and communication channels. Nonetheless, 6% of businesses still perceive this responsibility to rest solely with the IT department or designated technology personnel, while 3% consider it to be the responsibility of the executive board or board of directors. (see Figure 9)

FIGURE 9: **Employees' roles in information security in businesses**



However, in-depth interviews with businesses and associations reveal that while many have taken information security measures, these measures are not yet effective and comprehensive due to the following reasons:

- Lack of Effective Data Backup Method: Data is usually backed up (on a yearly basis) to an external hard drive, which is then stored in an executive storage room. The method of using 3-2-1 backup (where important data should be backed up in three copies, on two different types of media, with one copy stored offsite) has yet to be understood and followed by most businesses in Viet Nam.
- Not Using Reputable Software: Companies utilize reputable software solutions from domestic providers for accounting, payroll, inventory management, and production management. However, they have not adopted integrated solutions from a single vendor due to the high costs associated with such comprehensive software suites.
- Limited Antivirus Software Installation: Antivirus software is installed only on certain computers, such as those used by accounting staff and executives.
- Shared Wi-Fi Access: Customers are allowed to use the company's Wi-Fi network for employees.
- Personal Computers: Employees are permitted to bring and use their PC at work.

- Software Updates: Software is updated according to the recommendations provided by the software solution vendors.
- Awareness and Guidance: Employees are informed about online and email fraud through company email systems and Viber/Zalo groups. However, there has been no regular in-person training sessions on these topics.
- Lack of Cohesive Data Security: Businesses often place emphasis on securing accounting data, without a comprehensive approach to safeguarding the security of customer, partner, and employee data.
- Confusion of the IT Department's Role: The IT department is perceived as being responsible only for installing and repairing machinery, rather than for cybersecurity and information security.
- Improper Assignment of IT and Information Security Responsibilities: Information technology and security responsibilities are assigned to staff who also handle administrative, accounting, or marketing duties, with no dedicated personnel for IT or information security.
- Confidentiality Agreements: Employment contracts for managerial positions (equivalent to division heads) include a confidentiality clause, but no separate Non-Disclosure Agreement (NDA).

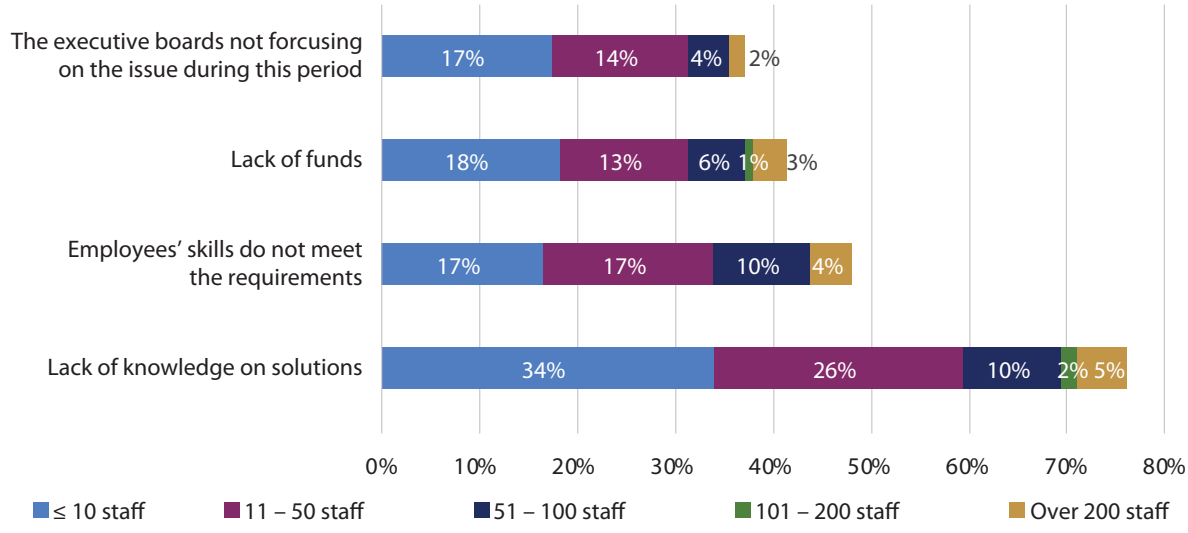
Lack of knowledge on proper solutions is the biggest obstacle in implementing Information Security in businesses

Reliable human resources, processes, and technology are all crucial factors for minimizing information security risks, in which most businesses reported facing obstacles. The biggest obstacle is a lack of knowledge about solutions (76%), followed by concerns about inadequate personnel capabilities (48%) and insufficient financial resources for investment (40%).

However, these obstacles can vary slightly across business sizes, the general issues remain consistent. One exception is that businesses with 101–200 employees cite only two obstacles: a lack of information about solutions (2%) and insufficient financial resources for investment (1%).

Ultimately, information security in any business relies on their highest management level. In the context of increasing risks, information security is not only an internal control issue but also a vital tool for building customer trust and achieving sustainable business growth. However, survey results reveal that 37% of business leaders have not prioritized information security at this stage. The reasons may include: (1) Leaders not recognizing the urgency of the issue, as 73% of businesses surveyed have not yet experienced any information security incidents; (2) The belief that many complexities can be avoided without implementing information security measures; (3) The perception that information security measures require more tasks, personnel, and costs without providing tangible benefits; (4) The assumption that small businesses with simple operations are not at risk. (see Figure 10).

FIGURE 10: **Challenges faced by businesses in implementing information security**



Information security training for all staff members is the top priority for businesses to prevent risks

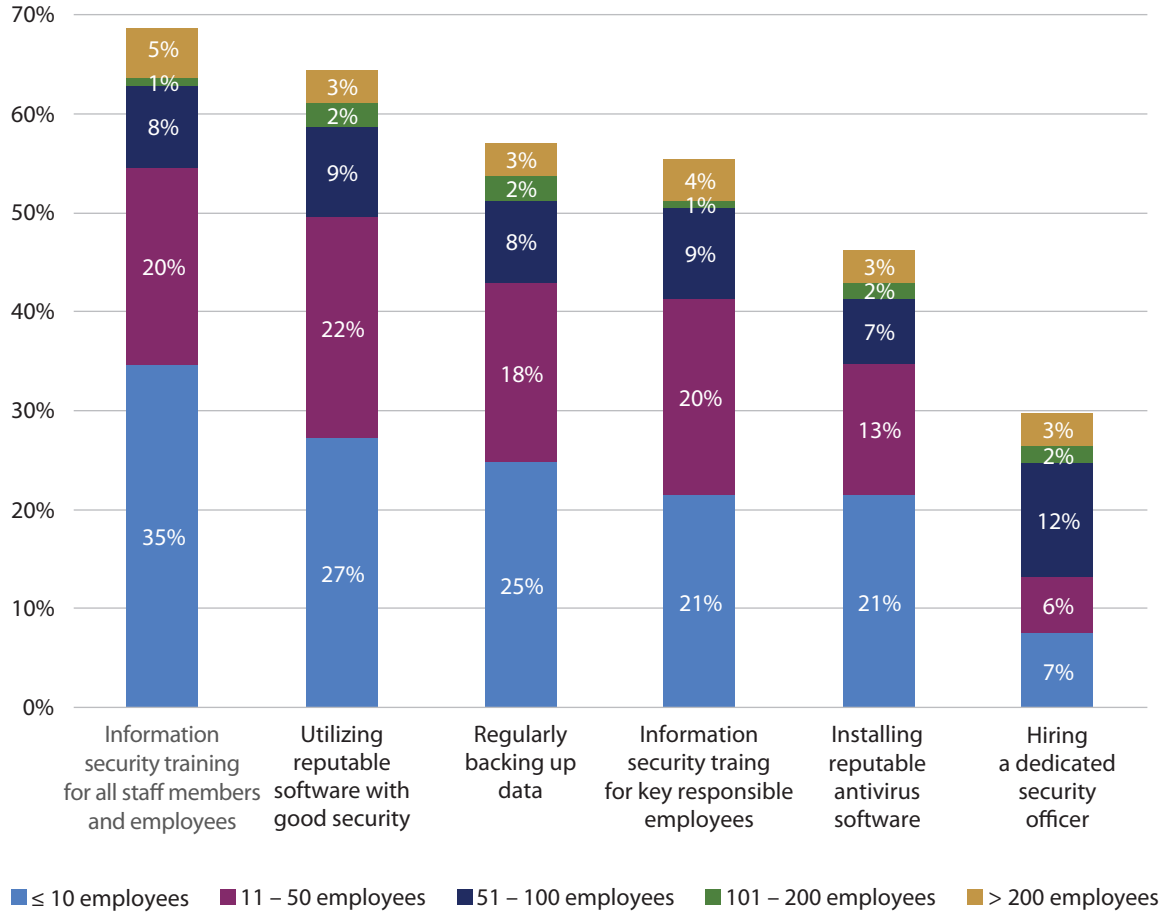
To explore businesses' information security plans in the near future, the consulting team put questions and proposed six basic solutions suitable for small and medium-sized, female-owned and led businesses to enhance information security. The six proposed solutions include:

- Information security training for staff with key responsibilities;
- Information security training for all staff members;
- Installing reputable antivirus software and firewalls;
- Using reliable, secure software;
- Backing up data on a regular basis (monthly/quarterly).
- Hiring/appointing an information security officer.

Overall, the most preferred solution is training all staff members in information security (69%), followed by using reputable, secure software (64%), regular backups (57%), and training key responsible staff (55%). Installing antivirus software and firewalls makes up 46%, while hiring a dedicated security officer is the least favored, with only 30% choosing this option (see Figure 11).

On the other hand, when categorized by business size, the preferred solutions show slight variations. Micro businesses (fewer than 10 employees) and large businesses (over 200 employees) prioritize information security training all employees. In contrast, businesses employing 11-50 or 51-100 people tend to favor using secure, reputable software. For businesses with 101-200 employees, four solutions are equally prioritized: using secure software, keeping data backups, training key responsible staff on information security, and hiring or appointing an information security officer.

FIGURE 11: **Preferred solutions to preventing information security risks in businesses**



48% of businesses have promulgated internal regulations on information security

Promulgating internal information security regulations is a critical and strategic step for any business, regardless of size. These measures not only safeguard valuable digital assets in the digital economy but also ensure legal compliance, enhance reputation, build customer trust, reduce risks, and create a secure, efficient work environment. According to the survey, 48% of businesses have issued internal policies for information security, while 52% have not yet taken this step (see Figure 12). Notably, 100% of large businesses have promulgated such regulations, and the larger the businesses are, the more they do this job. (see Figure 13).

FIGURE 12: **Percentage of businesses with internal regulations on information security**

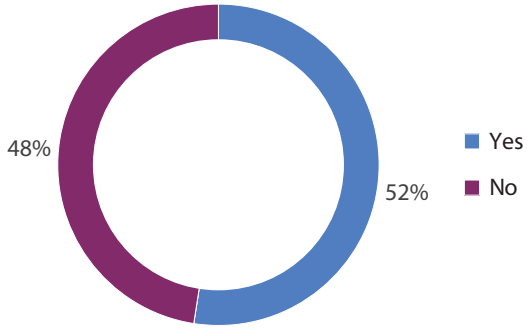
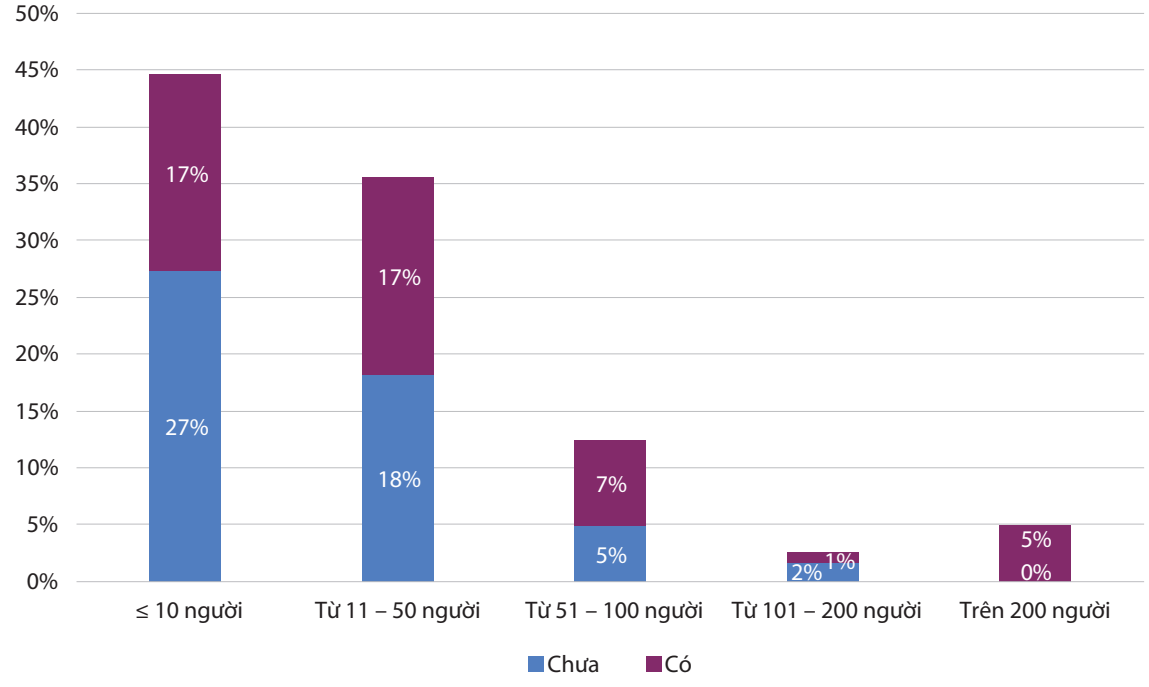


FIGURE 13: **Correlation between businesses' sizes and their promulgation of internal information security regulations**



2. Assessing Training Needs for Information Security in Digital Economy

2.1. For Association Organizations

In-depth interviews conducted with two associations in Hung Yen and Hai Duong provinces revealed that there are no existing reports assessing the training needs for information security in these localities. Additionally, the associations have not yet organized training sessions on this topic for their members due to limited capacity and resources, despite recognizing its current necessity.

All associations expressed a need for information security training for their members. 52% preferred a hybrid format (combining in-person and online sessions), 36% opted for in-person training, and only 9% selected fully online training. The preferred duration for in-person sessions was one day. (see Figures 14 and 15).

FIGURE 14: **Appropriate format of information security training (according to Association Organizations' opinions)**

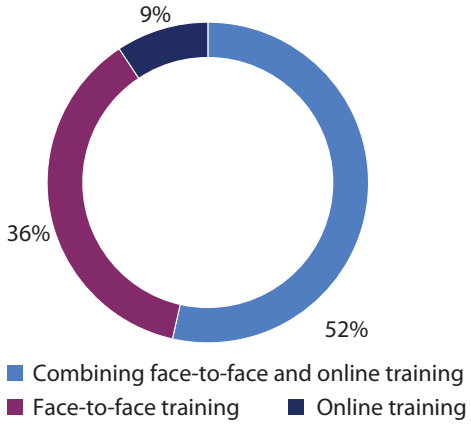
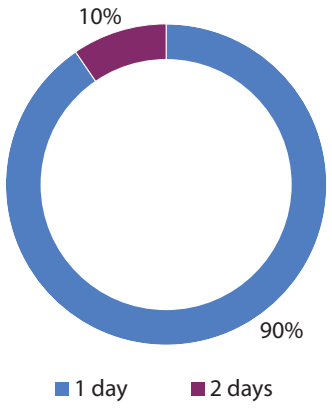
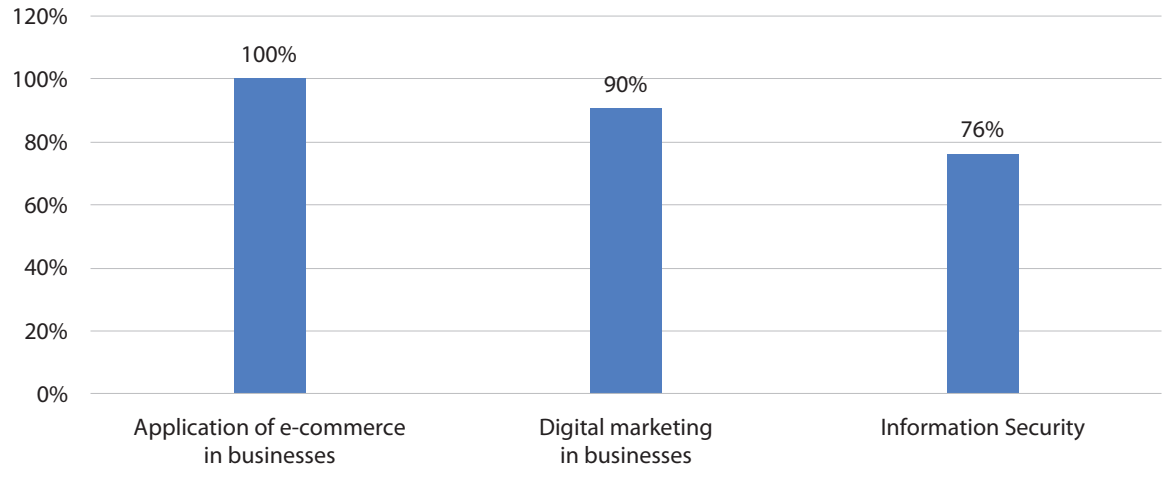


FIGURE 15: **Appropriate amount of time for information security training (according to Association Organizations' opinions)**



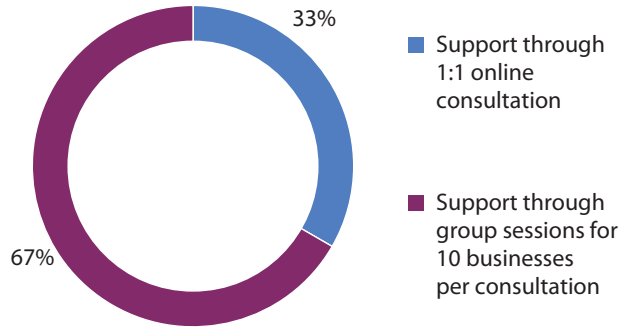
Statistically, 100% business members of Association Organizations expressed interest in learning e-commerce applications in business, with 90% of them wanting to study digital marketing, and 76% selecting information security as a key topic. (see Figure 16).

FIGURE 16: **Preferred training topics for Association Organizations' members**



Additionally, 100% of Association Organizations indicated that their members sought post-training support and among them, 67% preferred group support sessions for 10 businesses per consultation, while 33% favored one-to-one online consultation. (see Figure 17).

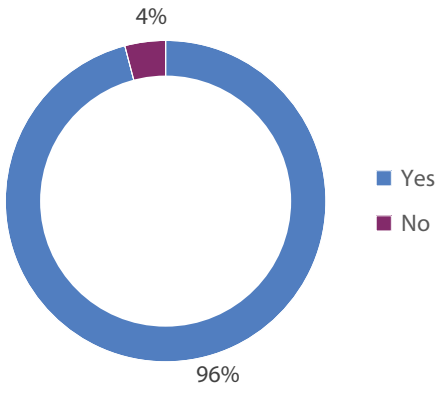
FIGURE 17: **Preferred post-training support format for Association Organizations' members**



Thus, based on Association Organizations' feedback, their members' training needs include:

- Topics: While information security is important, higher priority is given to e-commerce applications and digital marketing.
- Format: A hybrid approach (both online and in-person) is preferred.
- Duration: A one-day session is considered suitable.
- Post-training support: There is a clear desire for continued assistance after training.

FIGURE 18: **Businesses' needs of information security training in digital economy**



2.2 For Female-Owned and Led Businesses

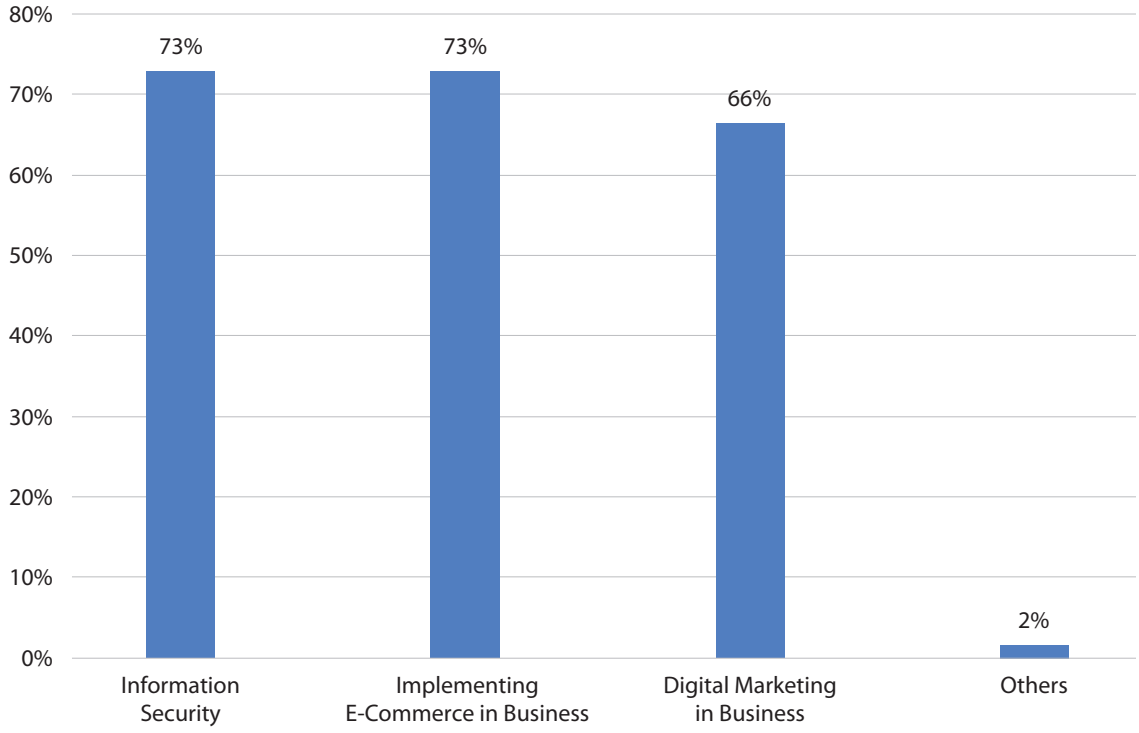
The majority of female-owned and led businesses express a strong need for information security training in the digital economy (96%). (see Figure 18).

Survey results show that when presented with three training topics, the highest choices were "Information Security" and "E-commerce Applications in Business," each selected by 73% of respondents. This reflects an increasing awareness among businesses about the significance of information security and the relevance of "E-commerce Applications in Business" to VCCI's findings, where market and customer acquisition challenges consistently rank among the top five difficulties faced by small and medium-sized enterprises in Viet Nam (PCI, 2020-2024).

Given the current digital economy, the shift of consumer purchasing behavior to online channels—especially after the COVID-19 pandemic—and the robust development of network infrastructure in Viet Nam, it is understandable that businesses prioritize these two topics. Additionally, 66% of businesses also selected "Digital Marketing in Business" as a training topic (see Figure 19), indicating significant interest in enhancing marketing capabilities in the digital environment.

There is a notable difference in training content preferences between the two groups: female entrepreneurs prioritize information security, whereas associations place the highest priority on e-commerce applications. This discrepancy may stem from differences in age and level of direct involvement in business activities.

FIGURE 19: **Businesses' preferred training topics**

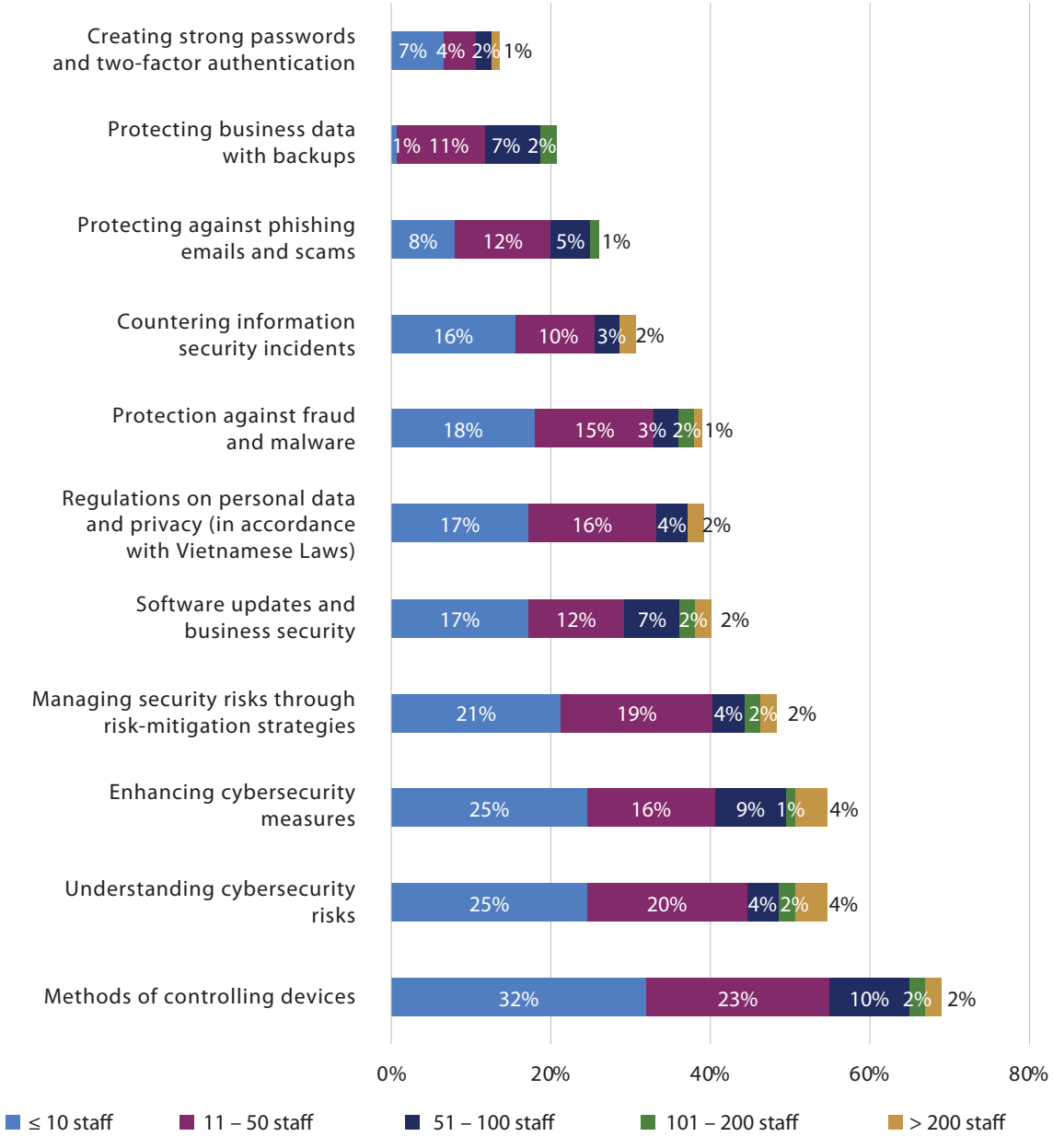


Female-owned and led businesses are mostly interested in how to control devices, applications, and accounts on both personal and business level

Based on content from GCA courses, the report's survey asked businesses to select up to five topics from a list of 11. The selection was designed to reveal the businesses' top priorities. The highest priority was how to control devices, applications, and accounts (67%), followed by understanding cybersecurity risks (56%), enhancing cybersecurity measures (55%), and managing information security risks through risk mitigation strategies (45%). Three other topics equally prioritized (40%) are protecting business data through backups; software updates and enterprise security; and compliance with regulations on personal data protection and privacy (as per Vietnamese law). The remaining four topics had lower selection rates: 39%, 30%, 26%, and 13%, respectively, including protecting against phishing and malware; incident response; protecting against fake emails and phishing; and creating strong passwords and two-factor authentication. (see Figure 20).

Notably, larger businesses prioritize two main topics: understanding cybersecurity risks (4%) and enhancing cybersecurity measures (4%). (see Figure 21).

FIGURE 20: **Training topics based on businesses' sizes**



Most of the surveyed businesses suggested that the appropriate amount of time for in-person training is one day (71%), while for online training, the preferred duration is half a day (62%)?. 29% of businesses suggested a two-day in-person training, combining classroom learning with a fact-finding visit to a business. Further investigation shows that the majority of those choosing the two-day format were micro and small businesses, reflecting their desire not only to update their knowledge but also to network and gain practical experience from other companies (see Figure 22).

FIGURE 21. **Appropriate amount of time for information security training**

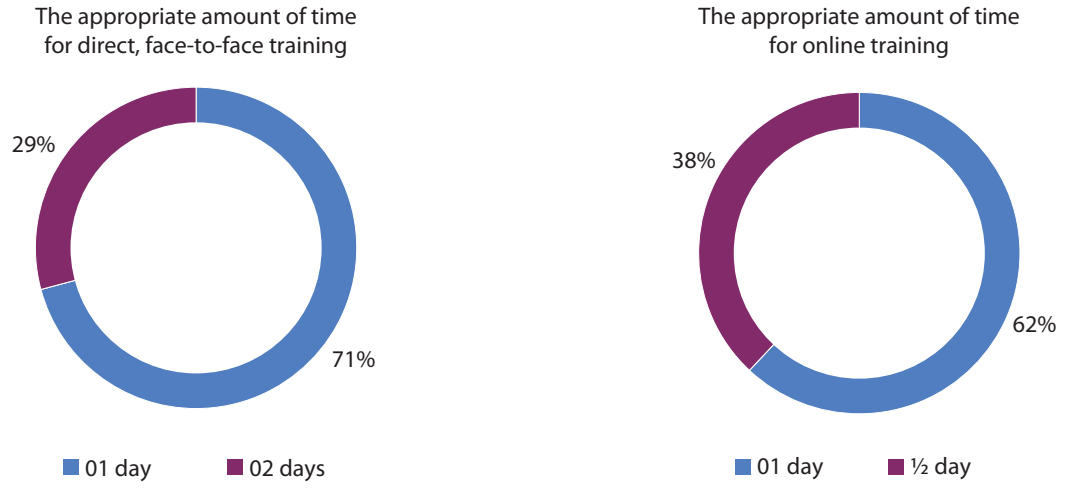
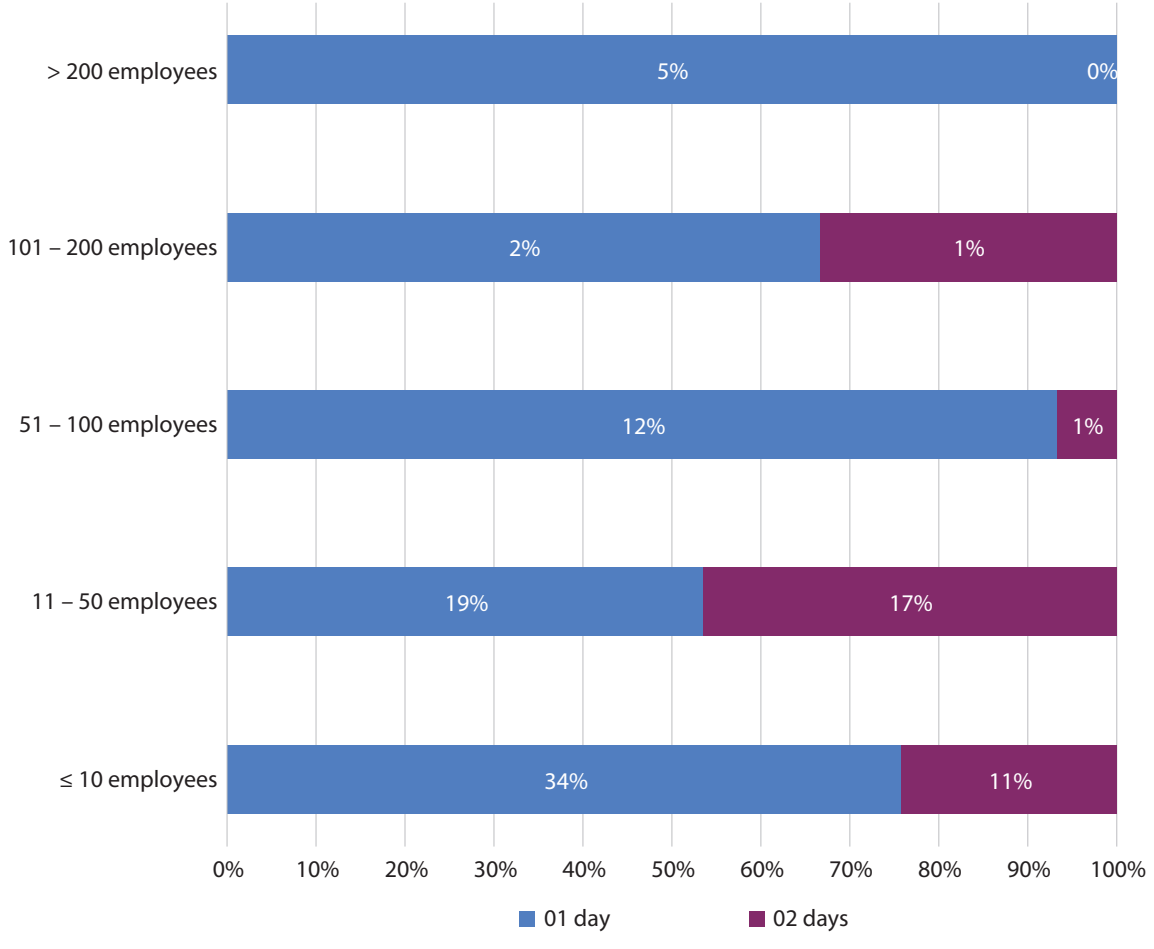
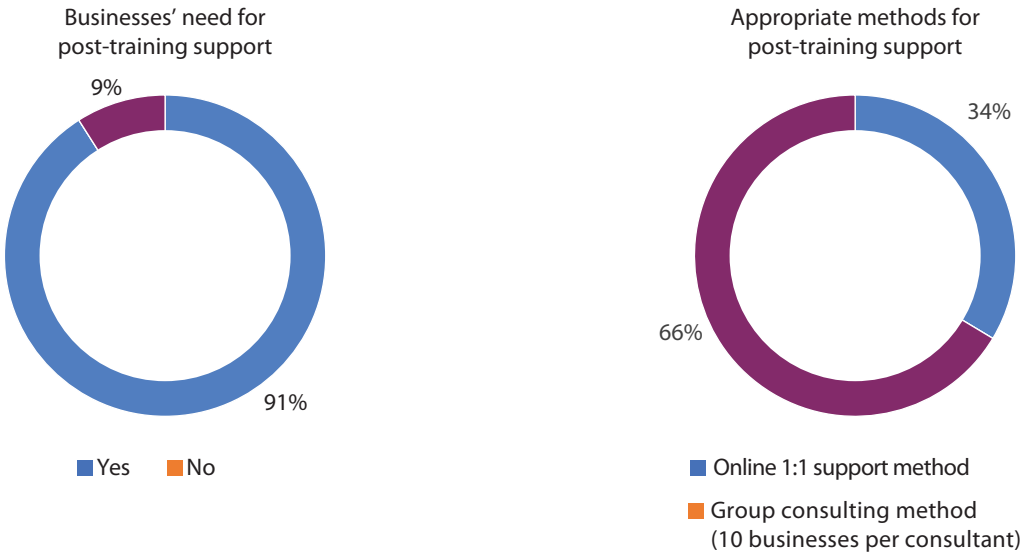


FIGURE 22: **Most appropriate amount of time for in-person training based on businesses' sizes**



Additionally, 91% of surveyed businesses expressed a need for post-training support, with 66% preferring group sessions for 10 businesses per consultation, and 34% opting for one-to-one online consultation (see Figure 23).

FIGURE 23: **Businesses' preferred needs and formats of post-training support**



In summation, the feedback from female-owned and led businesses indicates that many have a clear understanding of their responsibility for information security, recognize the obstacles to improving their information security posture, and demonstrate a strong demand for further training. These are positive signs, as once businesses are aware of the problem, they are more likely to seek resources, including participating in training programs, to address it effectively.

IV. Proposals on Information Security Training

1. For Association Organizations

Overall, the information security capabilities of these organizations are quite limited. The organizations themselves lack knowledge, strategies, and measures for protecting information security, and thus have not done enough to provide specific support for their members.

The methods of communication within an organization are relatively simple. They typically set up three Zalo groups: one for the board of directors, one for the executive committee, and one for all members to communicate about the organization's general activities, and share information about scams that female entrepreneurs may encounter.

Therefore

(1) There is a need to enhance the information security capabilities of the association organizations themselves.

(2) In addition to training on information security, associations should be guided on how to promote the necessity of information security, common risks, and common measures that small and medium-sized enterprises can apply to ensure information security. (These topics will be developed based on the training content provided by the project).

(3) Provide a set of visualized, simplified, and easy-to-understand materials for regular dissemination within Zalo groups and meetings. Given the project's limited resources, this could be a way to increase the sustainability of these activities.

General Proposal for VWEC Association Organizations: Provincial/city-level female entrepreneurs associations should have more comprehensive statistics on their members, such as business sizes and fields, and age of business owners, to better design organizational activities and support services for members.

2. For Female-Owned and Led Businesses

Currently, training services for small and medium-sized enterprises (SMEs) owned by women can be categorized into three groups based on the service provider: (1) free training services, (2) paid training services, and (3) training funded by state budgets.

(1) **Free Training Services:** These are usually organized by capacity-building projects and donors in collaboration with government agencies or female entrepreneurs' councils/associations. The participants include women with varying levels of education, skills, and training needs, leading to a lack of focus in the courses and insufficiently addressing the specific needs of individuals.

(2) **Paid Training Services:** These courses are typically provided by universities, female entrepreneurs' councils/associations, or training and education service companies.

However, these providers do not consider female entrepreneurs and female-owned and led SMEs as their main clientele, resulting in insufficient investment in researching and designing suitable training programs.

(3) **Training Using State Budget:** These training programs are funded by central and local government budgets. While the quality is gradually improving, the number of such programs remains limited.

The training contents usually revolve around basic and advanced knowledge in such business areas as finance, human resources, sales, and marketing; supplementary knowledge such as law, soft skills, digital transformation, and green transformation. However, there has not been enough investment in integrating gender factors or addressing the psychological and social barriers faced by women.

Traditional training methods do not fully match the conditions of female-owned and led SMEs. Specifically, the training is mostly conducted in traditional classroom settings, making it difficult for female entrepreneurs to absorb, interact, and practice. On that note, there is a lack of on-site training closely aligned with the actual conditions of the businesses.

Based on the results from the questionnaire and the current state of training for female-owned and led businesses as mentioned above, the consulting team proposes the following points:

3. Training Contents

(1) The course content should integrate information security topics with e-commerce applications and digital marketing in business;

(2) The training content on information security should cover all 11 modules, including: (understanding network information security risks; enhancing network information security; controlling devices, applications, and accounts of individuals and businesses; software updates & business security; creating strong passwords and two-factor authentication; protecting against phishing and malware; safeguarding business data with backups; protecting against spoofed and phishing emails; responding to information security incidents; managing security risks through risk mitigation strategies; and regulations on personal data protection and privacy). Priority should be given to the 7 modules of most interest to businesses: (controlling devices, applications, and accounts of individuals and businesses; understanding network information security risks; enhancing network information security; managing information security risks through risk mitigation strategies; protecting business data with backups; software updates & business security; and regulations on personal data protection and privacy as per Vietnamese law). However, it is advisable to select 2-4 modules for each course.

(3) Design questions on online platforms (such as Kahoot, Quizlet, etc.) before and after a training session to assess learning outcomes and help participants review key points, increasing their engagement and enthusiasm.

(4) During lectures, attention should be given to gender factors through examples, images, color usage, language, and form of address.

4. Organization Format

(1) Duration: One day for in-person courses with two instructors.

(2) Training Method: Use a learner-centered approach. The training should combine lectures with discussions and Q&A sessions. Classes should start at 8:00 AM and finish before 4:30 PM to allow participants to manage their personal schedules. Post-training support is essential, especially for micro-businesses (fewer than 10 employees) owned by younger women (under 30 years old), as these business owners are often busy and handle almost all business activities themselves, they have little time for self-improvement. Additionally, older female business owners (over 50 years old) may face challenges in accessing technology.

(3) Online Learning Duration: A maximum of 3 hours per session, considering time slots such as 2:30 PM – 4:30 PM or 8:00 PM – 9:30 PM.

5. Training Instructors

Qualified and experienced instructors are one of the key factors behind the success of training programs. Instructors should possess specialized knowledge, an understanding of women-led businesses, and practical experience.