International Journal of Multidisciplinary Research and Growth Evaluation.

Comparative analysis of information security policies at Big 4 Vietnamese logistics companies

Nguyen Xuan Quyet [1], Nguyen Hoang Tien [2*], Truong Kim Phung [3]
[1-3] Ho Chi Minh City University of Industry and Trade, Vietnam

* Corresponding Author: **Nguyen Hoang Tien**

Article Info

Abstract
Big 4 logistics companies in Vietnam (Leading companies in the field of logistics) show interest and play an important role in digital transformation. However, this is a process that is generating many difficulties and barriers. "Meanwhile, logistics businesses do not pay attention to the safety and information security of online platforms when only 5.26% of businesses believe that this is an obstacle to the digital transformation process of businesses," VLI Institute's research emphasized. The above survey results show that, in order to promote a strong digital transformation process, , there needs to be close cooperation between logistics businesses and partners in the entire service chain network to be able to make the right decision in choosing the appropriate application or platform. Digital transformation depends very much on much depends on the thinking of business leaders and must be considered as a strategy for businesses, including small and medium enterprises. From there, some solutions are proposed to improve preservation policies. Information security and factors affecting the security policies of Big 4 Logistic Companies in Vietnam.

Keywords: information security, comparative analysis, Big4, logistics, Vietnam

1. Introduction

Information security policy is an important factor in businesses. The goal of information security is to prevent threats from intrusions, cyber attacks, or unauthorized access to important information. By implementing strong and effective information security measures, organizations can keep their information safe and intact, protecting user privacy and critical business information. Information security in a business environment is the protection and maintenance of safety for important information, directly related to the operations, existence and development of the business. This is important because information in the business environment often includes human resource data, business strategies, customer and partner information, and many other important information. Information security ensures that this data is not lost, illegally disclosed, or modified without permission. When this information is protected, businesses can avoid negative consequences such as loss of important data, loss of reputation, or violation of legal regulations related to the protection of personal information. An effective information security policy and discipline in implementing information protection measures will help businesses prevent external threats, minimize cybersecurity risks, and increase trust. of customers and partners to businesses. This is very important to ensure the sustainability and survival of businesses in today's increasingly complex and competitive market.

Information security in businesses requires a combination of many important factors to ensure the safety and protection of important business information. Key factors such as absoluteness, integrity, availability and authenticity all play an important role in building an information security system for businesses. Karma.

Information security activities in businesses include preventing internal data theft, protecting transaction information with partners or customers, and protecting sensitive information such as personnel and strategic information. development strategy. This requires a combination of using modern tools and technology, implementing appropriate cybersecurity measures, along with training and security awareness for staff.

Information security is not just a process but a continuous and comprehensive effort to maintain security and protect critical business information against increasingly complex and advanced threats in today's environment. modern business school. Below we will understand the security policies at Big 4 logistics companies and propose key solutions on security policies in Vietnam.

2. Theoretical basis
The development of the global economy and diverse connections between countries have caused logistics to develop dramatically, while the application of information technology is one of the factors that increase the competitiveness of businesses in general. general and logistics enterprises (DNL) in particular. Therefore , DNLs must pay more attention to researching, applying and developing information technology and information security policies in their management activities. The article mentions a number of information technology trends that have been and are being applied in logistics activities, and at the same time proposes some policy implications to increase the use of technology and information security policies of companies. DNL at Big 4 Vietnamese logistics companies .

Securing information related to customers when cooperating to use the service is extremely important. This also affects customers' business processes, so DHD Logistics emphasizes security issues.

▪ Confidentiality of source information
Importing goods from reputable quality suppliers is an extremely big advantage in business. Not every seller has the ability to search, and it can take a lot of time and money.

We understand that only when source information is kept confidential can the cooperation between the two parties be strong. And DHD Logistics wants to aim for the long term. When customers mention DHD Logistics, everyone feels satisfied.

▪ Regulations on confidentiality of customer information of personnel
DHD Logistics strictly prohibits members of the Company from disclosing goods information and personal information about the Company's customers. Only with the Company's consent to serve the requirements of the competent authority. If information is leaked to the outside, that person will take full responsibility. DHD Logistics stops cooperating with that employee immediately.

We are a unit with many years of operation in the field of Logistics, understanding issues related to customer information. Committed to absolute security, storing information on secure software.

▪ C is committed to protecting customers' personal information
The personal information of members of our company is committed to absolute confidentiality by our company according to our company's personal information protection policy. The collection and use of each member's information is only carried out with that customer's consent, unless otherwise prescribed by law.

Do not use, transfer, provide or disclose to any third party the member's personal information without the member's consent.

In case the information server is attacked by hackers leading to loss of member personal data, our company will be responsible for reporting the incident to the investigating authorities for timely handling and notification. let members know.

Absolute confidentiality of all members' online transaction information, including digital accounting invoice information and documents on our company.

Our company management requires individuals when registering/purchasing to provide complete relevant personal information such as: Full name, contact address, email, phone, ... , and is responsible for the legality of the above information. Our company management board is not responsible nor will we resolve any complaints related to that member's rights if it considers that all of that member's personal information provided upon initial registration is incorrect.

▪ Smart Email Security for Logistics Enterprises
Email is always the main means to help businesses connect with each other, but some rules for using email when sending and receiving users are still not really safe, making businesses easily encounter dangerous email attacks. and suffered a lot of damage. Especially businesses with a large number of employees such as Logistics companies.

Difficulties in securing Logistics business emails
- Users set passwords that are too simple and do not change their passwords regularly
- The number of employees is large, but the awareness base of users' email security is not large enough.
- If you use poorly secured business email services, there are often countless potential risks and dangers for Logistics businesses such as: Spam, Email Virus in the inbox but not warned to users. Mail Server systems often encounter problems, often encounter errors in sending and receiving mail.
- The ability to target targeted business email attacks is becoming easier and easier today.

Digital Shadows' analysis shows that breaking into business emails is not difficult but causes extremely serious damage.

In 2018, Digital Shadows found more than 12.5 million business emails for sale online, including user names, passwords and owner profiles, causing about 12 billion USD in damage to businesses.

Digital Shadows also discovered that groups of cyberattackers on businesses only need to hire a number of outside hacker units for $150 for each hacked business email account.

▪ Vietnamese logistics businesses have not focused on information security
According to a recent survey by the Vietnam Logistics Research and Development Institute (VLI), Vietnamese businesses do not pay attention to the safety and information security of online platforms. Only 5.26% of businesses believe that security neglect hinders their businesses' digital transformation process.

VLI Institute's survey results show that 38.24% of logistics businesses believe that COVID-19 has created the need for digital transformation, while 42.65% of businesses believe that the impact of COVID-19 is the main impact. is to change customer needs (such as using more electronic transactions, e-commerce delivery services...) in addition, there are other

trends formed such as changing the concept of things. running a logistics business, the ability to work remotely.

Businesses participating in the survey expressed interest and evaluated the important role of digital transformation, however, this is a process that is generating many difficulties and barriers.

These include technological compatibility between your business and partners in the logistics service chain (44.74% of businesses), limited funding and limited human resources (42.11% of businesses). find suitable transformation technology (39.47% of businesses) and 28.95% of businesses wonder how to spend appropriate investment funds and how to start in the process. digital conversion.

In addition, converting huge amounts of existing information to digital platforms is also an obstacle for 15.97% of businesses.

"Meanwhile, logistics businesses do not pay attention to the safety and information security of online platforms when only 5.26% of businesses think this is an obstacle to the transformation process. enterprise numbers", VLI Institute's research emphasized.

The above survey results show that to promote strong digital transformation, there needs to be close cooperation between logistics businesses and partners in the entire service chain network to be able to make the right decisions. in choosing the right application or platform.

Digital transformation depends greatly on the thinking of business leaders and must be considered a strategy for businesses, including small and medium enterprises.

In fact, logistics businesses have the characteristics of operating with large-scale data (big data), the number of orders can be from several hundred thousand to millions of orders/day, the need for digital transformation becomes important. an urgent issue and a prerequisite for carrying out the activity.

One thing worth noting is that although there are many difficulties affecting the application of information technology and digital transformation of Vietnamese logistics businesses, businesses have made great efforts to invest and apply information technology. Necessary information in performing key logistics services.

Specifically, 75% of businesses are using FMS (delivery management software); 63.89% of businesses are using OMS and WMS software (order management software, warehouse management software); 61.11% of businesses are using TMS (transportation management software).

There are very few applications that can optimize operations such as VRP (vehicle routing system) or automatic storage and retrieval system AS/RS, automatic guided vehicle (Automatic guided vehicle). Enterprises use it at a rate of 19.4%, 16.67% and 11.11%, respectively.

In particular, the application of drone technology has not been used at all, but up to 11.11% of Vietnamese logistics businesses plan to use it in the future.

3. Research Methods
Information security policy is extremely important and necessary for every business. In today's globalized economy, information is considered vital for businesses. However, many businesses are still not aware of the importance of information security and the possible risks from information leakage within their own businesses. According to statistics on information security from TÜVRheinland Vietnam Certification Organization, each year over 15,000 hospital

records are found in the trash, and 30,000 passwords of Internet accounts are found. was published online, 25 people from this company's business development department moved to a rival company, banks had to pay millions of dollars due to an attack on the business transaction system and 300,000 credit account numbers. Personal belongings were stolen, some were published on the Web. Information security must be considered a management and business responsibility, not simply a technical factor that should be left to technology experts or the IT department. To ensure business security, a business must understand both its problems and the solutions to the problems. Therefore, applying information security management systems is a very important job for businesses in the current era of globalized economic integration. An information security management system is part of a comprehensive management system in an enterprise, mainly approaching business risks to establish, implement, operate, monitor, review, and maintain. Maintain and improve information security. The information security management system includes organizational structure, policies, planning activities, responsibilities, practices, processes, methods and resources. Not only is there the misconception that "information security is an issue that needs attention for IT managers and IT departments", but many businesses also have other "serious" misconceptions. That is the way of thinking that security threats coming from outside are the biggest risks; Information security only aims to ensure the protection of information technology systems and infrastructure; Human resource management in information security is not as important as technology; Applying high-tech and advanced solutions will increase security. Meanwhile, information security management issues with personnel, policies and management systems are not applied. The solution that many large companies in the world are currently applying is the information security management system (ISMS). ISMS is offered not only as a solution to demonstrate its function as an information security tool with a 4-step cycle (design, implementation, monitoring and maintenance) but also to contribute to change. Misconceptions about current information security in businesses. Some Vietnamese businesses are also currently applying this solution as a measure to enhance their security in the era of global integration. On the other hand, "ISMS is not limited to the management of information processed by electronic means but can also be information in other forms such as information written on paper, stored in electronic file format. electronically, sent by post, email or communicated verbally. ISMS is part of a comprehensive management system within an enterprise, primarily a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security. believe. Thus, the management system includes organizational structure, policies, planning activities, responsibilities, practices, processes, methods and resources. But the essence of all the above problems is the human factor. When businesses ignore this factor, no matter how much they invest in technology, the risk of information leakage will still occur and affecting production and business is inevitable." - said Mr. Hans - Joachim Roderfeld, a provider of ISMS solutions. For Vietnamese businesses, there are still no specific regulations from the authorities. But in general, a transparent privacy policy usually has all of the following elements:

- Personal information that the organization collects
- Purpose of collecting the above information

- How to organize and use information
- How is that information shared?
- Partners can share information
- Right of choice for users
- Other information

To build a reasonable privacy policy, organizations need to determine the types of information they collect, which typically include: name, age, gender, SDT, bank card, cookies (for web browsers).), IP address, onsite time, fingerprint,... Businesses today tend to collect as much customer information as possible. This is a misconception. More information means more difficult security, higher risk of data breach attacks. Another important factor is disclosure about sharing: will user information be shared with third parties? If so, in what cases? Who is responsible when a data breach occurs ? A reasonable security policy will help businesses minimize the risk of being attacked by cybercriminals in any form. This is not only true from the customer perspective, but also true for Investors. In a flat world with a competitive economy, businesses need to shape their brand as a "trusted" brand before being able to carry out other PR campaigns. Hopefully, after this article, readers can build reasonable security policies for businesses, respecting customers to minimize risks when security incidents occur.

4. Research results and discussion
- **Research results**

An enterprise information security policy is a document that explains how a business collects, stores, manages, uses, and shares information of employees, partners, customers... Currently, it is still There are no specific regulations on what an appropriate information security policy is. Therefore, businesses often build their own policies. A reasonable and effective security policy often includes elements such as: How to collect information; The types of information the organization has collected; Purpose of collecting information; How the organization uses information; Scope of information sharing; How that information is shared; Subjects with shared information; Other information. Information security policy in the enterprise. Currently, there are many ways for businesses to build information security policies. Businesses can use pre-written privacy policy templates shared on websites, then further edit them to suit their business. It can be seen that information security plays an extremely important role in business operations. Therefore, the security process requires to take place strictly and effectively.

Information security policy
1. Purpose and scope of collection
The main data collection on the company's website includes: full name, email, phone, customer address in the contact section. This is the information that the company needs members to provide when submitting account registration information or wanting to purchase and use the company's services.

Members will be responsible for the security and storage of all service usage activities under the information they provide and their email boxes.

2. Scope of information use
The company uses the information provided by members to Contact to confirm orders and contact delivery to members when receiving requests from customers;
Provide product information to customers if requested by the customer;
Send marketing and promotional emails about goods provided by the company;
Send notifications about company website activities;
Contact and resolve with users in special cases;
Do not use users' personal information other than for confirmation and contact related to transactions at the company;
When there is a request from a judicial agency including: Procuracy, Court, police investigation agency related to certain law violations of the customer.

3. Information storage period:
Members' personal data will be stored until the administrator requests cancellation or there is a customer's consent to cancel. In all other cases, member personal information will be kept confidential on the company's server.

4. Methods and tools for users to access and edit their personal data
Members have the right to self-check, update, adjust or cancel their personal information by contacting the company website administrator to do this.
Members have the right to submit complaints about information security content, please contact the Administration Board of the company website. When receiving this feedback, the company will confirm the information. In case the member's feedback is correct, depending on the level, the company will take timely measures.

5. Commitment to protecting customer personal information
's members' personal information is committed to absolute confidentiality according to the company's personal information protection policy. The collection and use of each member's information is only carried out with that customer's consent, unless otherwise prescribed by law.
- Do not use, transfer, provide or disclose to any third party the member's personal information without the member's consent.
- In case the information server is attacked by hackers leading to loss of member personal data, the company will be responsible for reporting the incident to the investigating authorities for timely handling and notification to the authorities. known members.
- Absolute confidentiality of all members' online transaction information, including digital accounting invoice information and documents on the company.
- The company management board requires individuals when registering to purchase products to provide all relevant personal information such as: Full name, contact address, email, phone, etc., and take responsibility. Responsible for the legality of the above information. The company management board is not responsible nor will it resolve any complaints related to that member's rights if it considers that all of that member's personal information provided upon initial registration is inaccurate.

6. Mechanism for receiving and resolving customer complaints

When a customer has a complaint, the customer can send the complaint via the Company's email or send it directly to the company's address.

Any controversy, claim or dispute arising from or related to the transaction or these Regulations and Conditions will be resolved by negotiation, conciliation, arbitration and or Court according to Law protect consumers

Enterprise information security process

Corporate information security often goes through 4 basic steps as follows:

Step 1: Data encryptionData encryption is the transformation of information from one form to another. This process is quite complicated and requires a lot of specialized knowledge. This can limit illegal access to information. + Step 2: Set a strong password This is the step to directly protect business information. Because if you don't use hacking tricks, only subjects who know the password can log in to get information.+ Step 3: 2-step authentication Businesses can install 2-step authentication function to increase security, meaning that in addition to data encryption and password settings as above, other information can also be used to log in to the place where confidential information is stored. + Step 4: Secure the LAN system against outside access. This network system is used to connect computers within a small range to share information with each other via files or some other devices. Because it allows connection to other computers, it does not exclude the possibility of external access to the network system. Therefore, businesses need to strictly manage to ensure high safety.

Commitment to information security after leaving the job

Commitment to information security after the employee leaves the job is as necessary as commitment during the working period. This commitment is made in a written document clearly recording the commitment between the employee and the employer that the employee shall not disclose or make public the confidential information of the enterprise after they Leave work, unless requested by a competent state agency, to absolutely protect information within the business.

In addition to the methods mentioned to avoid the situation of business information being disclosed to the outside through the business's employees, there are also methods of information confidentiality and non-competition agreements.

Confidentiality and non-compete agreement

A non-compete and confidentiality agreement (often called an NDA) also commits employees not to disclose business information to third parties. The confidentiality and non-compete agreement includes the following basic issues: regulations on confidential information; security scope; confidentiality period; obligations of employees; Responsibility for breach of agreement...

Discussion
What does corporate information security include?

Information safety and security plays a particularly important role in businesses and organizations because it plays a role related to the survival of these organizations and businesses. Currently, information security in businesses includes activities such as:

+ Prevent theft or copying of internal data
+ Prevent hackers' actions such as identity theft and installing malware on business systems
Ensure data exchange, online business, and transactions in the safest state
All information related to operations, finance, personnel, transactions, and customers needs to be kept absolutely confidential by relevant departments.
Enterprise information security meets 4 factors: confidentiality, availability, integrity, and non-repudiation.

Current information system security issues in Vietnam

Information security, information security in businesses, system security , app information security, software information security are concepts that have recently begun to be interested in Vietnam. Most users are not clearly aware of the role of information security. That is also the reason why thousands of identity cards, degrees, card numbers... were made public.

Understanding the risks of information security, application programmers and information protection specialists are trying to access new technology to upgrade the "protection barrier" for individuals and organizations .

At large systems, there will be an IT Security team specializing in providing incident response plans as well as establishing risk management tools to control the situation.

However, that is still not enough, the number of new systems on the market in recent years has grown extremely fast while the infrastructure in Vietnam is not enough. This is the new challenge we are facing.

5. Conclusion and recommendations
Conclusion

BIG4 in Vietnam all have something in common are: global, requires high skills, good English, quite high odds. However, each company has a very different culture, pursues different core values, and competitive benefits.

Globalization and digital transformation in the fields of production, service and life have brought challenges and opportunities for the Logistics industry. Therefore, smart logistics is the optimal solution to handle the increasing complexity and volume of activities. Technologies such as the Internet of Things (IoT), information communication technology (ICT) and artificial intelligence (AI) allow logistics activities to be handled effectively and maximize resource savings.

In recent years, Vietnam's economy has witnessed rapid growth in the e-commerce market (81% in 2020). It is this rapid and rapid growth that has opened up many strong development opportunities for the Logistics service industry. Currently in Vietnam, there are over 4,000 domestic Transportation and Logistics companies providing diverse and comprehensive services from goods transportation procedures to tax payment or payment..., we can see countless job opportunities that Logistics brings. The strategy for the coming years will focus on globalization, digitalization, e-commerce and sustainability with a customer-centric focus.

Challenges posed in the process of digital transformation of the Logistics industry.

In addition to the opportunities, current digital transformation efforts in the logistics field show some basic difficulties and challenges as follows:

Financial

Enterprises providing logistics services are small-scale enterprises with weak financial resources. On average, the process of digital transformation for an entire enterprise has a total cost of about 200 million to tens of billions of VND, which is not suitable for small and medium enterprises.

If businesses decide to invest in automation like foreign models, it will cost initial investment, but if they follow the internal model, it will cost information technology human resources and take a lot of time.

Basically, it will be extremely difficult for logistics providers to carry out digital transformation without support from the State or financial and credit institutions.

About technology

Logistics is considered a key industry in international trade, so logistics digital transformation needs to be carefully invested in to quickly adapt to the current market context. However, the level of application of science and technology in Vietnam is still not high, businesses only apply it individually and are not synchronous. International standard software has not been widely applied in Vietnam

Basically, businesses just stop at digitizing and storing electronic data and have not really connected the ability to look up data or process orders on online platforms.

About competition

Currently, when competing with large logistics service providers in the world, Vietnamese businesses still reveal many problems. These include: Weak financial potential, outdated technology, and lack of high-quality human resources. In addition, there are other reasons such as: lack of management skills, cumbersome apparatus, lack of synchronization, etc. Many Vietnamese businesses are facing challenges and fierce competition from the market. Foreign enterprises, with experienced units, the ability to provide services and better financial potential...

Thus, to be able to gradually transform digitally in businesses providing logistics services, each business needs to gradually overcome the difficulties mentioned above. At the same time, be clearly aware that digital transformation is inevitable if you do not want to be eliminated from the market:

- Digital transformation must be solid, following a suitable roadmap with a long-term plan, and careful in each step such as process selection,
- Look for suitable suppliers in terms of both reputation and quality.
- When digitally transforming in the logistics field, there needs to be a synchronous transformation. It is necessary to build a digital platform for the logistics service chain, helping to connect stakeholders in the chain (ports, carriers, agents forwarding companies, warehouses...) to share data and increase visibility for the chain, improving efficiency.

Digital transformation solutions for the Logistics industry in 2023

Currently the logistics industry is facing difficult problems related to weak financial potential, outdated technology, and lack of high-quality human resources for digital transformation. Understanding the difficulties and ready to accompany businesses, FSI - Vietnam's leading digital transformation solution provider has researched and developed the comprehensive large data storage and processing platform FSI Data Platform.

FSI Data Platform will solve the problem of lack of modern technology because the software supports Logistics businesses in creating databases throughout the goods transportation process. Based on advanced technology such as machine learning (ML), deep learning, artificial intelligence (AI), etc. The process of creating a large database thus becomes fast, accurate, and economical save time and costs.

FSI Data Platform supports agencies, units in the logistics industry and customers to link and effectively utilize data resources in the digital environment.

Limit

Smart Email Security for Logistics Enterprises. To ensure customers' trust in the company regarding confidential information.

Email is always the main means to help businesses connect with each other, but some rules for using email when sending and receiving users are still not really safe, making businesses easily encounter dangerous email attacks. dangerous and suffered a lot of damage. Especially businesses with a large number of employees such as Logistics companies.

Difficulties in securing Logistics business emails

- Users set passwords that are too simple and do not change their passwords regularly
- The number of employees is large, but the awareness base of users' email security is not large enough.
- If you use poorly secured business email services, there are often countless potential risks and dangers for Logistics businesses such as: Spam, Email Virus in the inbox but not warned to users. Mail Server systems often encounter problems, often encounter errors in sending and receiving mail.
- The ability to target targeted business email attacks is becoming easier and easier today.

Commitment to protecting customer personal information

- Customers' personal information is committed to absolute confidentiality according to the company's personal information protection policy. The collection and use of each customer's information is only carried out with that customer's consent, unless otherwise prescribed by law.
- Do not use, transfer, provide or disclose to any third party the customer's personal information without the customer's consent.
- The company will provide some information such as: name, address, phone number to the shipping service when using invoice and contract delivery services for customers.

Provide information, services and support according to your requests Send emails to notify typical programs and events.
- Resolve disputes and problems arising related to the use of international express delivery services.
- Prevent illegal or prohibited activities as outlined in the Terms of Service.
- Measure and improve company services.
- company will be responsible for reporting the incident to the investigating authorities for timely and timely handling. will also notify customers in the most clear way.

▪ Absolutely secure all customer online transaction information, including digital invoice and accounting information.

Build good relationships with customers
▪ Customer service in Logistics is an issue that many people are concerned about. Meeting customer needs is always the top priority for businesses.
▪ Loyalty and the rate of customers using the service again will be a measure of success in the field of customer service. In general as well as customer service in Logistics in particular.
▪ For companies, they consider customer service in Logistics as an essential and important activity that they provide and if done well, they can win the trust of customers and get long-term contracts to smooth and sustainable business.

Request
Deputy Director of the Import-Export Department (Ministry of Industry and Trade) Tran Thanh Hai said that a very clear trend today in the logistics industry is investing in technology and digital transformation in logistics service businesses. Businesses in the industry need to clearly see the trend of applying information technology, scientific and technological achievements, and artificial intelligence in order management, transportation management, and seaport management.

Another trend is greening the supply chain, which means businesses must meet requirements for reducing emissions, being environmentally friendly, meeting the requirements of commercial activities in the coming period and all other All participants in the logistics supply chain must meet greening requirements, from green transportation, green packaging, green warehousing, green logistics data management...

For the logistics industry to develop, infrastructure is an extremely important factor. In the past two years, many key infrastructure projects, important highways, and regional connections have been built and completed.
▪ Vietnam's goal is to complete 3,000 km of highways by 2025, and by 2030, complete 5,000 km of highways.
▪ Along with that are coastal roads, airports, seaports.

These are necessary and sufficient conditions for Vietnam to develop the logistics industry in the future. However, to achieve the goal of cutting logistics costs, improving the business environment, and enhancing the competitiveness of the logistics industry in the context of international economic integration and the fourth industrial revolution, we also have to many works to do.
-First, we must continue to improve policies and laws on logistics services. Amend and promulgate new policies and laws regulating logistics services, multimodal transport cross-border transport, comprehensively covering logistics services, and legalizing international commitments on logistics.
-Second, the State needs to improve logistics infrastructure, continue to review master plans and plans, ensure synchronization of transportation infrastructure and transportation services with the goal of developing the logistics service industry. . Attract investment in large-scale, centralized, regional logistics centers to help store and preserve goods for long periods of time, thereby spreading distribution flows to different places.

Third, to build human resources in the logistics field in Vietnam, requires the active participation and commitment of relevant parties, including the Government, local authorities, and logistics companies and vocational schools.
In particular, to accurately determine labor needs and recruitment, the State needs to develop vocational standards for the logistics field and support schools to invest in facilities and equipment in the field logistics.
Fourth, on the logistics businesses side, it is necessary to build business strategies, implement strategic alliances, joint ventures with partners or merger and acquisition activities to create strong businesses and increase sales competitiveness.
Deputy Minister of Planning and Investment Tran Duy Dong said that with the synchronous and effective implementation of the above solutions, Vietnam's logistics industry will develop even stronger in the future.

References
1. Luu Quang Trung. Russia-Ukraine war and risks to global supply chains. International journal of mechanical engineering. 2022; 7(7):663-640.
2. History of formation | Faculty of Management - University of Economics Ho Chi Minh City (ueh.edu.vn)
3. Goal | Faculty of Management - University of Economics Ho Chi Minh City (ueh.edu.vn)
4. Training Program | Faculty of Management - University of Economics Ho Chi Minh City (ueh.edu.vn)
5. Anh DBH, LDM Duc, PB Ngoc. Subjective Well-Being in Tourism Re¬search. Psy¬chology and education. 2021; 58(5):3317-3325.
6. Bien BX, Tien NV. Solutions enhancing competitiveness of made-in Vietnam brands in Vietnamese market, International Journal of Research in Marketing Management and Sales. 2019; 1(2):93-99.
7. Diem PT, Vu NT, Nhan VK, Vang VT. The Strategy of CRM System Development ment at ¬Mega Market Vietnam. Inter¬national jour¬¬nal multidisciplinary research and growth evaluation. 2021; 2(4):802-806.
8. Diem PT, Vu NT, Dung HT, Dat NV. The Process of CRM System Implemen ¬tation at Dien May Xanh in Vietnam. Inter¬national journal multidiscip¬¬linary research and growth evaluation. 2021; 2(4):761-768.
9. Diem PT, Vu NT, Dung HT, Bien BX, Duc PM. Customer Care and Customer Relation ¬ship Maint enance at Ministop, Family ¬Mart and CoopSmile in Vietnam. International jour¬¬nal multidiscip¬¬linary research and growth evaluation. 2021; 2(4):744-751.
10. Diem DL, TTT Trang, PB Ngoc. Development of Tourism in South Central Coastal Provinces of Vietnam. Jour¬nal of archeology of egypt/egyptology. 2021; 18(8):1408-1427.
11. Diep LH, Vu DT Hai, TTH Thuan. China and USA in Vietnam's International Relations in the Region. Jour-nal of archeology of egypt/ egyptology. 2021; 18(8):2681-2710.
12. Duc LDM, Thuy Cooperative, Yen NTH. Corporate Social Responsibility and Corporate Financial Performance Case of Listed Vietnamese Companies, Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie. 2018; 32:251-265.
13. Duc LDM, Mai NP. Enhancing Sustainability in the Contemporary Model of CSR: a Case of Fast Fashion Industry in Developing Countries. Social Responsibility Journal, 2020.

14. Dung HT, Tien NV. Branding building for Vietnam tourism industry reality and solutions, International Journal of Research in Marketing Management and Sales. 2019; 1(2):63-68.
15. Dung NTH, TT Trang, VT Hien, Editor Phuong. Factor Affecting Tourists' Return Inten ¬tion. A Case of Binh Quoi Village in Ho Chi Minh City. Jour¬nal of archeology of egypt / egyptology. 2021; 18(9):493-507.
16. Dung NTH, TT Trang, PB Ngoc. Assessing Customer Satisfaction for Can Gio Tourist Destination in Ho Chi Minh City. Journal of archeology of egypt/egyptology. 2021; 18(14):249-268.
17. Giao NQ, TTT Trang, NP Mai. Sustainability Issues in the Development of Higher Education Industry. Hong kong journal of social sciences. 2021; 57:79-90.
18. Hung NT, Vu NT, Bien BX. Risks of Vietnamese Enterprises in Trade Relations with China. International Journal of Research in Finance and Management. 2020; 3(1):1-6.
19. Mai NP. Green Entrepreneurship Understanding in Vietnam. International Journal of Entrepreneurship, 2020, 24(2).
20. Minh HTT, Dan PV. Branding building for Vietnam higher education industry-reality and solutions, International Journal of Research in Marketing Management and Sales. 2019; 1(2):118-123.
21. Minh NH Diep, LH Vu, DT Hai, TTH Thuan. ASEAN and China in Vietnam's Inter¬national Relations in the Region. Jour¬nal of archeology of egypt/ egyptology. 2021; 18(8):2661-2680.
22. Ngoc PB, TTT Trang. Current Path to Community Based ¬Sustainable Tourism Development of Khanh Hoa Province in Vietnam. Jour¬nal of archeology of egypt / egyptology. 2021; 18(9):508-525.
23. Tran Thanh Toan. Opportunities and challenges for quality of human resource in public sector of Vietnam's logistics industry. International journal of public sector performance management", 2022. https://doi.org/10.1504/IJPSPM.2025.10056383