Journal of Network and Information Security
9 (2) 2021, 42-50
http://www.publishingindia.com/jnis

The Need and Impact of Implementing an Effective Virtual Private Network (VPN) in the Retail Business Sector during COVID-19 Pandemic

Pritam Kumar
Lecturer, Digital Business Management, Martin de Tours School of Management and Economics, Assumption University, Thailand. Email: pkumar@msme.au.edu

Abstract: As a result of digitalization, retail organisations have more freedom and opportunities to reduce the cost of transitions, capture many new customers, maintain positive relationships with current customers, and provide positive energy and motivation to employees by offering a variety of benefits such as work from home and remote working, as well as allowing consumers to purchase goods and services from any location [1]. When employees are working or when customers visit the retail business network, the retail business is concerned with maintaining a secure connection [2]. Most employees and consumers use computers and mobile devices for work, so they require a secure connection as well as protection against the sharing of sensitive information and data [3]. The purpose of this study is to examine the factors that influence the adoption of virtual private networks in the retail industry using secondary data. According to the findings of this study, Virtual private networks (VPNs) are necessary for providing secure connections over public networks. There are numerous factors that have an impact on the adoption of virtual private networks in retail businesses to create a risk-free and secure network. These factors are both direct and indirect. Virtual private networks (VPNs) not only provide security for network and data access, but they also assist in keeping the data that is made available safe and secure.

Keywords: Digitalisation, E-Commerce, Retail business, Security, Virtual Private Network (VPN).

I. Introduction

The issue of COVID-19 is expected to have a significant impact on the entire human race and their way of life, as well as on businesses, particularly retail businesses, in general. It helps to accelerate the improvement of the virtual private network in the retail business environment. In this pandemic situation, most retail businesses have turned to virtual private networks to help them grow their businesses [4]. The time spent on a virtual private network has increased significantly since the outbreak of the COVID-19 virus. The adoption of virtual private networks was influenced by several factors, including data security, cyber-attacks, networking infrastructure, and so forth. To reach the greatest number of consumers and employees during this uncertain period, the retail industry required a virtual private network. Virtual private networks (VPNs) for retail businesses required increased concentration on the data security provided by them, particularly after the acquisition of work from home capabilities, e-commerce platforms, digitalisation, and increased time spent on networking infrastructure [5]. Following the implementation of COVID-19, most retail businesses have opted to use private networks rather than public network operations.

As reported by Forbes [6], virtual private networking (VPN) services provide security and privacy to more than 400 million businesses and consumers around the world. Virtual private networks (VPNs) play a significant role in protecting the information of employees and customers that is received and sent through the internet and e-commerce platforms, respectively. It aids retailers in protecting their internet connections from unauthorised users and cybercriminals such as hackers.

The demand for remote accessibility in the retail industry is a driving force behind the development and expansion of the company in the market. In this pandemic time, everyone wants to be safe and have easy access to their workplace. A better virtual private network was required by the retail industry, but a lack of expertise in virtualization has hampered the growth of both the business and the virtual private network. The adoption of private clouds, on the other hand, has increased the use of virtual private networks, and it is anticipated that the use of virtual private networks in retail businesses will grow

significantly after COVID-19 [7]. There are several factors that influence the adoption of virtual private network market in retail business, including increased data security issues, advanced and critical cyber threats, increased use of wireless devices within organisations for work.

According to Allied Market Research [8], the global virtual private network market was valued at 25.41 billion dollars in 2019 and is expected to grow to $75.59 billion dollars by 2027. In addition to providing secure communication for connecting group members using public telecommunication infrastructure, virtual private networks also assist in maintaining privacy using security procedures and the tunnelling protocol (also known as VPN). To ensure maximum privacy, virtual private networks (VPNs) establish encrypted and secure connections. Following the COVID-19 pandemic, retail businesses have resorted to using virtual private network solutions. It directs the global virtual private network market to increase the demand for delivering a secure work culture and remote workplace in order to allow employees to work from their homes. It increases the number of data breaches and makes it easier to access digital media outlets, news, and content in different parts of the world.

II. Research Goals/Objectives of the Study

The primary goal of this study is to determine the impact of the implementation of an effective virtual private network in the retail industry.

A) Secondary Objectives

- To understand the information provided by virtual private network.
- Investigate the viability of a virtual private network for retail business transactions.

B) Research Methodology

According to the findings of this research study, various factors that influence the adoption of virtual private networks are evaluated. This study makes use of secondary data such as published research papers, news articles, and blogs that are related to virtual private networks and the various factors that influence the adoption of virtual private networks in general.

III. Literature Review

A study conducted by D. C. Chou [9] examines the use of virtual private networks in e-commerce transactions. The primary goal of this research was to discover the wide range of content available through virtual private networks. Another goal of this research was to determine the significance of virtual private networks in e-commerce dealings and transactions as a secondary objective. It had investigated a variety of virtual private network concepts and searched for various technologies for virtual private networks, which were then compared to one another. A virtual private network (VPN) was examined in this study to determine its suitability, capability, advantages, and limitations at a time when electronic commerce was being adopted and implemented. This study made use of economic analysis to compare the benefits and costs of virtual private networks at the early stages of their implementation in organisations. The findings of this study reveal the benefits and drawbacks of using virtual private networks for electronic commerce transactions to conduct business. A practical example of technology is provided in the economic analysis at the time of deciding on whether to implement a virtual private network. In addition, this study discusses the strategic and practical implications of virtual private network technology.

Tarek S. Sobh and Yasser Aly [10] investigate how a virtual private network (VPN) can be used to connect to a public network via the internet. A virtual private network (VPN) is also available to them as an advantage. According to the findings of this study, virtual private networks (VPNs) are the most useful for sharing and exchanging small amounts of data through encrypted tunnels. The organisation shares a small amount of data with the help of a web-based system in the shortest amount of time possible while maintaining a high level of security.

Marcia Mkansi [11] stated that recurring costs were the most significant component of online trading, and that small businesses faced a variety of challenges to reduce the costs associated with digitalization. The qualitative approach is used in this study, which includes a multi-case study. The various electronic retail strategies for smooth e-commerce transactions are investigated in this study through the lens of the technology-organization-environment theoretical framework. Specifically, the findings revealed that the adoption cost of technology, organisation, and environment strategies in utilising to minimise the cost barrier was the lowest of the three. All these strategies were beneficial in terms of lowering costs and increasing the overall efficiency of the organisation.

IV. Impact of Adoption of Effective Virtual Private Network in Retail Business

As a result of recent developments, retail businesses are being prepared not only for the urban environment, but also for small towns and rural areas. Following COVID-19, it is anticipated that the retail industry will grow rapidly and gain a significant share of the market. Because of COVID-19, it is expected that retail market share will increase, and there will be significant development and opportunity in e-commerce and digitalization.

The digital platform provides better opportunities for retail businesses to gain access to new markets around the world as well as new customers and clients. E-commerce platforms not only provide better products and services at the lowest possible price or cost, but they also aid in the reduction of operational costs. During and after COVID-19, most retail businesses will use the remote working concept and work from home facility to make working more convenient for their employees, which will help to increase employee motivation. All these factors have a positive impact on the adoption of virtual private networks, which assist in providing internet users with greater safety and security.

V. Aspects/Factors of Major Influence as Regards to VPN

- *Increasing Internet, Mobile, and Wireless Device Usage, as well as Social Media Users:* Today's workers can access business applications and connect to retail business networks from any location by using the internet, tablets, mobile applications, laptops, smartphones, and netbooks. Because the world is suffering from a pandemic, most workers can connect to retail business networks from any location. To connect with customers and employees, retailers are incorporating digitalization and internet-based transactions into their operations [4]. Most retail businesses are utilising low-cost data plans and mobile devices to facilitate remote working. When employees are working or when customers visit the retail business network, the retail business is concerned with maintaining a secure connection. Most employees and consumers use computers and mobile devices for work, so they require a secure connection as well as protection against the sharing of sensitive information and data. It is necessary to have key components in virtual private networks (mobile, computer, and other wireless devices virtual private networks) and other security products to increase the security and transparency of devices used in the workplace. If it is possible, retailers use mobile devices, computers, laptops, and other wireless devices to complete their tasks while on the go. The retail industry uses a variety of apps, the internet, and websites to promote products and services to customers. All these considerations had a direct impact on the adoption of virtual private networks [12].
- Bringing Your Own Device (BYOD) policies are being implemented by most retailers in order to reduce costs while also improving employee performance and productivity. As a result, workers have been using their own devices, such as laptops and smartphones, to complete their tasks. It increases the number of devices in the workplace or the number of devices on the retail business network, and it increases the need for device and data security because of this increase. Authenticating that remote workforce is securely connected to retailers' network using employees' own devices (private networks) ensures that remote workforce is protected from a variety of cyber-attacks by retailers. During COVID-19, retail businesses have been subjected to face a variety of challenges and issues that will affect their ability to maintain continuous operations and interact with employees, customers, and other stakeholders. Because of the ease of access, most retail businesses use an internet-based operating system. The revenue generated by the internet and the revenue generated by retail businesses are closely related. In recent years, most retail businesses have become connected to the World Wide Web [13]. Most retail businesses make use of e-commerce and remote working. Wireless technologies, such as those employed by COVID-19, help to increase internet access. Smart phone users use the internet to do their shopping and to share any data or information they might have. As a result, m-commerce is growing rapidly. Consumers take advantage of mobile shopping during and after COVID-19, and the use of the internet for data sharing and the purchase of any product or service with a single click increases significantly. However, it also observes that an insecure network poses a variety of risks, with hackers, unauthorised users, and third-party users being able to gain access to sensitive information and misuse it [14]. As a result, not only is it dangerous for consumers, but it is also dangerous for retailers, who must protect their networks from all possible attacks and risks. Most retail businesses use virtual private networks to create a secure network and to conduct business over the internet.
- *Advanced and Challenging Cyber Security Threats***:** Millions of retail businesses provide their employees with the opportunity to work from home. Using the internet and wireless devices, workers connect to the organization's network and use both private and public networks to complete their work tasks. The internet also provides the capability of increasing worker connectivity as well as their overall productivity. A universal platform is being used to conduct transactions on the internet, which has become increasingly popular and vast in scope [15]. Shopkeepers are extremely concerned about unauthorised access to, and hacking of, public and organisational networks. For target consumers and businesses, hackers and attackers scan some public networks, as well as corporate networks, for information. The attackers use the internet for fraud and theft. The

threats to internet-based crimes and cybercrimes are becoming more complex, and hackers are employing more advanced technology in their hacking and attacking efforts. Finding and solving the theft that has taken place through hacking and cyber theft is not easy. Most of the time, it is difficult to recognise, and it takes more time to track down the actual crime and the perpetrators of the crime. Cyber criminals take advantage of insecure internet connections to conduct their operations. Previous studies have revealed that cyber criminals can easily gain access to third-party networks and that they can easily connect through unsecured connections, Wi-Fi, and hotspots, whereas organisations do not have adequate security measures in place to protect their internet and network connections, according to the findings.

- Retail businesses, as well as all parties involved in transactions, face numerous issues and challenges because of a lacklustre defence strategy. Retailers and consumers should investigate secure networks and connections to conduct secure transactions using public networks and outside corporate networks, as suggested above. Cyber criminals, attackers, or hackers are constantly on the lookout for new vulnerabilities to exploit to attack and hack information, while retailers are on the lookout for secure connections that do not require attack or hacking [16]. To achieve this, retail businesses use virtual private networks and encryptions to improve security. They also implement various strategies and policies to prevent cybercrimes and attacks from occurring. It was discovered in this study that the use of a virtual private network is essential for reducing hacking and other internet attacks. All these considerations have a direct impact on the adoption of virtual private network technology.
- *Digital Infrastructure and Industrial Revolution:* Retail businesses require digital infrastructure for e-commerce and mobile commerce, as well as the ability to work remotely. Because digitalisation and the use of the internet generate and collect vast amounts of data from real-time information, businesses require analytical data to make significant and effective decisions. Customers, suppliers, and other stakeholders provide retailers with a variety of data. Retailers store raw data in databases, analyse the data, and then use the information for proper operation [17]. The retail industry has had to deal with new technology and a revolution in the business world. The new industrial revolution takes advantage of the digital world and real-time data, as well as access to new sources of information. To improve business operations, it provides new analytics tools for businesses such as predictive learning algorithms, scenario analysis, and visualisation, among other things. With the introduction of new technology and tools, it is now possible to access a wide range of data from both public and private networks via wireless connections. Product and service delivery to consumers are transformed by the digital revolution and Industry 4.0, which also support supply chain operations, customer relationship management, production, and marketing departments. The development of digital infrastructure and the industrial revolution have made it possible for various facilities to connect with the global market using the internet and the World Wide Web [18]. It also provides connectivity to public and private networks, and most retail businesses now rely on digital platforms for e-commerce and, more recently, m-commerce transactions to succeed. However, connecting to public networks has some limitations and drawbacks. Without proper care and security, connecting to both private and public networks can be dangerous, as can connecting to unsecured networks. Thus, for improved workplace performance, it is critical to use secure connections and networks. Then a proper virtual private network is required for the retail business.
- *Remote Accessibility***:** Retail businesses affected by the COVID-19 pandemic have already begun the process of shifting their operations to digital transformation, concentrating on operating their businesses digitally and accepting new network changes. When a retail business decides to allow its employees to work from home, virtual private network connections are required. Then the retail business must implement a virtual private network, and the first stage of the information and technology team must be established to allow for virtual workforce [19]. Then the retail business provides employees with unrestricted access to ensure that they can perform their jobs properly and effectively. However, the virtual private network connection is the most important process for gaining access to data at any time and from any location. Retail businesses provide their employees with the ability to log on from any location and any time during this pandemic, and retail businesses also provide the ability to access the network via the internet and other wireless technologies during this period. Most organisations have adopted Bring Your Own Device (BYOD) policies, which allow employees to connect to and access the organization's network by using their own devices. Employees use wireless devices to connect to the organization's network and digital technologies to download various files and data from the network using their mobile phones.
- Retail business workers use a variety of applications to complete their tasks; however, as technology advances, it is becoming more accessible to all types of devices, including computers, and smart phones, among others

[20]. Because most applications are available on mobile, smart phone, and wireless devices, retail businesses can use them to increase the number of employees who are available for remote working. These applications improve the efficiency and productivity of employees, but they require security and authorization access to avoid causing a variety of problems in the workplace. Consequently, the adoption of a proper virtual private network by the retail industry is required to provide secure access of various working applications and organisational networks.

- *Enhanced Safety and Security***:** Antivirus protection and firewalls are used by retail businesses to provide secure internet connections to customers. Only antivirus and firewall software are effective in protecting against and preventing hacking, attack, and cybercrime. Many antivirus programmes are actively engaged in the battle to save and safeguard important information from viruses, malware, and other types of viruses [21]. They assist the system in protecting the organization's network from malware and known viruses, but they do not provide comprehensive protection; rather, they only assist in keeping the system up to date. Many public networks are not secure for the exchange of information, and even connecting to these networks creates several difficulties and problems for the proper operation of devices. When a retail business does not have enough capital to invest in security measures, it will implement some antivirus and firewalls, but this will not provide complete security. The retail business provides a virtual private network as well as data encryption. Client information, sensitive customer information, trade secrets, internal communication, and internal documents are all protected by using a virtual private network. Because retail businesses are small and have limited operations and connections, they can get away with using encryption and other network protection systems [22]. However, if a retailer has large operations and obtains a large amount of data, it must use virtual private networks to secure connections and protect against risk, cyber-attack, and hacking.
- *Encryption Transfer, Interchange, and Exchange***:** Even though retail businesses have a significant market share and operations, they face a variety of challenges and issues related to the sharing and exchange of information over a secure network in the COVID-19 pandemic. VPN is used by retail businesses for secure and safe information and data sharing with people within and outside of the organisation. This includes people within the organisation like employees, managers, and colleagues, and people outside of the organisation like suppliers, the government, consumers, and other stakeholders. Virtual private networks (VPNs) are the network technology of choice for most businesses, depending on their needs [23]. To ensure the security of data transfers, retail businesses use virtual private networks (VPNs) and encryption to connect public networks and private networks to securely share their organization's internet connection.
- A virtual private network and encrypted data are required when a retail business must upload, download, and transfer valuable information as well as share it with others using the mail, a storage device, and an outsider's network from the retail business. Authentication is provided for every transaction using encryption and decryption. It means that only authorised and authentic individuals can gain access to the file using the appropriate encryption key and decrypt the data using the appropriate decryption key. The use of a virtual private network, on the other hand, is critical to improve the security of information transfer, sharing, and exchange between inside and outside parties. All these security considerations have an impact on the decision to use a virtual private network.
- *Availability with Remote Data Access***:** A virtual private network (VPN) service for retail businesses provides remote connectivity to connect securely with the host server to access the data and information [24]. A virtual private network connection for a retail business provides end-to-end encryption, protecting data from being accessed from a remote location or by prying eyes. A virtual private network (VPN) for retail businesses is a smart alternative and choice for retail businesses that require high levels of security while also providing accessibility for employees. Remote working and remote data access facilities provide a convenient way to gain access to necessary data from any location and at any time [25]. If a device is stolen, remote access provides a hostage facility. If a device is stolen, a virtual private network provides access to cloud computing and a secure connection.

  If a company requires powerful computing capabilities as well as secure remote access, it should consider implementing a virtual private network.
- *Strategic Distancing from International Censorship:* If a country implements internet censorship, it will impose some restrictions on the flow of information from that country. When employees travel and work in locations where there is internet censorship, it can have a negative impact on the efficiency and effectiveness of executives and other employees [26]. Most virtual private network service providers display a list of places and locations from which organisations can choose fast speeds and connections to the company's internal network. Retail businesses can choose from a variety of locations and settings in which to display their business network. To

conduct international business, retail businesses must establish a connection with the internet through their home country network. Specific countries prohibit the use of certain applications, search engines, and network systems, but retail businesses are required to use certain applications and products [27]. When using a secure virtual private network, it is possible to connect directly to a virtual private network location and access the product and services offered there. Retail businesses require search functionality that is not restricted by censorship.

- *Establishment and Associated Costs***:** To integrate a traditional retail business virtual private network into an organization's current network, a significant amount of effort, energy, and time is required. Users of retail businesses, the number of servers required to provide virtual private network access to users, and the budget and financial condition of the organisation determining whether to implement a virtual private network are all factors in determining which type of virtual private network to use [28]. The acquisition of an appropriate virtual private network, whether with or without the presence of an existing information technology department, is therefore a very difficult task for small retail businesses [29]. When the cloud virtual private network is expanded, retail businesses find it difficult to meet the business needs of virtual private networks at a lower cost, and retail businesses must set aside time and money to do so. Although virtual private networks (VPNs) are the most important component in data and network security, there are some disadvantages to using a business or corporate virtual private network. The adoption of virtual private networks has a direct impact on the cost of setting up the network [30]. Budget and financial constraints confront medium and small retail businesses when attempting to implement an appropriate virtual private network [31].
- *Management and Operations:* The data generated by every retail business, including information about customers, competitors, distributors, and the supply chain is enormous. Because this data is an asset of the retail business, it is critical that it is kept secure and safe. It creates a variety of risks and insecurity if the retail business does not manage all this data. As a result, most retail businesses employ virtual private networks, encryption methods as well as providing employees with training programmes to help them manage risks and uncertainties. For retail businesses to manage their valuable data with the appropriate security and encryption provided by virtual private networks, they must first implement a virtual private network.

VI. Findings and Conclusions

A virtual private network (VPN) is a critical technology for establishing an encrypted connection between two computers in a secure network. The primary advantage of a virtual private network is that it provides an appropriate level of security for connecting systems of all types and sizes. Retailers have tremendous opportunities to build customer-centric business models to improve operational efficiency in this digital age, according to the National Retail Federation.

By implementing digitalization, they can respond more quickly to customer demands and make work more convenient for employees by utilising a remote working model. As a result of the COVID-19 pandemic and its aftermath, retailers have encountered intense competition not only between individual and domestic retailers, but also with a broader constellation of alliances that the retail businesses have developed within their own network. Retailers make extensive use of private and public networks to reach the greatest number of customers and employees. It can sometimes result in serious problems, such as the hacking of personal and valuable information, or the misuse of data obtained from a third party. Because of this, it is necessary to provide appropriate security and protection for all transactions and data sharing. It is possible to connect remote users to a company's network using a virtual private network, which makes use of a public network infrastructure such as the Internet to provide secure access. A retail business connects remote users' mobile or computer devices to a virtual private network gateway on the retail business network, which requires the authentication of the device and then creates a network link and sends it back to the device that authorised it to extend the internal network to the remote users. Without the use of a virtual private network, the network of POS terminals and computers used by retailers and consumers is at risk of being compromised and unsafe. Some web threats, such as web attacks and data hacking, are encountered by users. Every day, internet users are confronted with millions of critical threats, all of which have a significant impact on their ability to work efficiently and effectively. As a result, every internet user requires security when using the internet and electronic media for sharing and purchasing purposes. It is difficult to defend oneself against cybercrime. Client network servers, POS terminals, and computers are all protected by using virtual private networks (VPNs). As a result, it helps to keep customers' personal information and valuable information safe from hackers and other third-party users.

A virtual private network (VPN) allows users to connect to a private network in a private and secure manner using the internet. It makes use of an encrypted connection, referred to as a virtual private network tunnel. It is a location where all internet communication and traffic are managed through the use of appropriate security measures. In this digitalization era,

it has been observed that data security threats are becoming increasingly complex and advanced, as well as an increase in data security treatments. The use of wireless devices and mobile technology within organisations is a major factor in the growth of the virtual private network market. The demand for remote accessibility among users drives the market's expansion. When it comes to virtual private networks, expertise in virtualization is required; however, when this expertise is not available, retail businesses suffer losses of valuable data and information, as well as trust. The COVID-19 pandemic has had a significant impact on consumer behaviour and preference, and all these factors have had a direct impact on the retail industry. Most consumers prefer privacy and avoid social interaction. Shopping is done online, and employees require a safe environment to work in as well. Retail businesses must develop their own capabilities to track consumer behaviour and manage demand across the entire supply chain. The online and digital platforms are becoming increasingly important in comparison to the tried and tested formatted channel.

VII. Recommendations

In this pandemic situation, online shopping and working from home can be simple and safe. However, consumers and employees alike require security and safety when engaging in e-commerce transactions. They must safeguard their personal information and data against unauthorised users and rogue networks. To accomplish this, the proposed retail business should make use of virtual private networks to encrypt data and conceal IP addresses. When it comes to the selection and implementation of virtual private networks, retail businesses should opt for the most secure protocol available. As a result of the pandemic situation, retail businesses should implement virtual private networks to conduct more secure electronic commerce transactions.

VIII. Practical Implications

Retailers will benefit from the findings of this study because it has some practical implications. This study assists retailers in implementing virtual private networks, as well as identifying the benefits and drawbacks of conducting e-commerce transactions. It provides accurate information to make an informed decision about the selection of a virtual private network and helps to improve the performance of e-commerce businesses. This research is used by retail businesses to make decisions about which virtual private network to use to provide secure remote working access to their employees. These studies allow its employees to work from home while maintaining a high level of security and protection. Mobile devices and computers are connected to the business network via a virtual private network, and employees of retail businesses and consumers can access and use this network for secure working and purchasing or for sharing information over the public Internet. Consumers can gain access to retail business networks while maintaining complete security and data protection using virtual private networks.

IX. Managerial Implications

The purpose of this study is to investigate the various factors that have an impact on the adoption of virtual private networks and technology. The findings of this study make it simple for managers to understand the benefits and drawbacks of using a virtual private network for their retail business. This research will also assist managers in making a variety of decisions regarding security and privacy issues relating to electronic commerce and transactions in general.

The study also contains fundamental information about virtual private networks, including the benefits they provide to retailers, employees, and customers.

References

[1] L. McGregor, and N. Doshi, "How to make your team motivated, remotely," *Harvard Business Review*, 2020. [Online]. Available: https://hbr.org/2020/04/how-to-keep-your-team-motivated-remotely

[2] D. Gilmore, "9 ways to make your company network secure," 2019. [Online]. Available: https://tdwi.org/articles/2019/04/23/dwt-all-9-ways-to-make-your-company-network-secure.aspx

[3] N. Lord, "An expert guide to securing sensitive data: 34 experts reveal the biggest mistakes companies make data security," 2021. [Online]. Available: https://digitalguardian.com/blog/expert-guide-securing-sensitive-data-34-experts-reveal-biggest-mistakes-companies-make-data

[4] OECD, "OECD policy responses to corona virus (COVID-19), e-commerce in the time of COVID-19," 2020. [Online]. Available: https://www.oecd.org/coronavirus/policy-responses/e-commerce-in-the-time-of-covid-19-3a2b78e8/

[5] UNCTAD, "Digital economy report 2019, value creation and capture: Implications for developing countries," 2019. [Online]. Available: https://unctad.org/system/files/official-document/der2019_en.pdf

[6] Forbes, "What is a business VPN, and how can it secure your company?," 2018. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2018/11/15/what-is-a-business-vpn-and-how-can-it-secure-your-company/?sh=38169dc563a5

[7] IBM Cloud Education, "Virtual private could," 2019. [Online]. Available: https://www.ibm.com/cloud/learn/vpc

[8] Allied Market Research, "Virtual private network market by component (solution and services), type (remote access VPN, site-to-site VPN, and others), deployment (cloud and on-premise), and end user (commercial users and individual users): Global opportunity analysis and industry forecast, 2020-2027," 2020. [Online]. Available: https://www.alliedmarketresearch.com/virtual-private-network-market

[9] D. Chou, D. Yen, and A. Chou, "Adopting virtual private network for electronic commerce: An economic analysis," *Industrial Management and Data Systems*, vol. 105, pp. 223-236, 2005, doi: 10.1108/02635570510583343.

[10] T. S. Sobh, and Y. Aly, "Effective and extensive virtual private network," *Journal of Information Security*, vol. 2011, no. 2, pp. 39-49, 2011, doi: 10.4236/jis.2011.21004. Published Online Jan. 2011. [Online]. Available: http://www.SciRP.org/journal/jis

[11] M. Mkansi, "Ebusiness adoption costs and strategies for retail micro businesses," *Electronic Commerce Research,* 2020. [Online]. Available: https://doi.org/10.1007/s10660-020-09448-7

[12] A. R. Locket, "Online marketing strategies for increasing sales revenues of small retail businesses," Ph.D. dissertation, Walden University, 2018. [Online]. Available: https://scholarworks.waldenu.edu/dissertations

[13] W. Reinartz, N. Wiegand, and M. Imschloss, "The impact of digital transformation on the retailing value chain," *International Journal of Research in Marketing*, vol. 36, no. 3, pp. 350-366, Sep. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167811618300739

[14] N. Giandomenico, and J. de Grooto, "Insider vs. Outsider data security threats: What's the greater risk?," 2020. [Online]. Available: https://digitalguardian.com/blog/insider-outsider-data-security-threats

[15] McKinsey and Company, "Digital globalization: The new era of global flows," 2016. [Online]. Available: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx

[16] N. Lord, "Social engineering attacks: Common techniques and how to prevent an attack," 2020. [Online]. Available: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

[17] S. S. Darvazeh, I. R. Vanani, and F. M. Musolu, "Big data analytics and its applications in supply chain management," 2020. [Online]. Available: https://www.intechopen.com/chapters/69320

[18] N. Ndung'u, and L. Signe, "The fourth industrial revolution and digitization will transform Africa into a global powerhouse," 2020. [Online]. Available: https://www.brookings.edu/research/the-fourth-industrial-revolution-and-digitization-will-transform-africa-into-a-global-powerhouse/

[19] Cameron Camp, "As the COVID-19 pandemic has many organizations switching employees to remote work, a virtual private network is essential for countering the increased security risks," 2020. [Online]. Available: https://www.welivesecurity.com/2020/03/18/work-home-how-set-up-vpn/

[20] L. Silver, A. Smith, C. Johnson, J. Jiang, M. Anderson, and L. Rainie, "Use of smartphones and social media is common across most emerging economies," 2019. [Online]. Available: https://www.pewresearch.org/internet/2019/03/07/use-of-smartphones-and-social-media-is-common-across-most-emerging-economies/

[21] N. J. Rubenking, "The best antivirus protection for 2021," 2021. [Online]. Available: https://in.pcmag.com/antivirus-from-pc-ma/34241/the-best-antivirus-protection-for-2020

[22] S. Ursillo, C. Arnold Jr., "Cyber security is critical for all organizations - large and small," 2019. [Online]. Available: https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small

[23] P. Renjen, "The heart of resilient leadership: Responding to COVID-19," 2020. [Online]. Available: https://www2.deloitte.com/us/en/insights/economy/covid-19/heart-of-resilient-leadership-responding-to-covid-19.html

[24] D. Janssen, "VPN explained: How does it work? Why would you use it?," 2021. [Online]. Available: https://vpnoverview.com/vpn-information/what-is-a-vpn/

[25] L. Spawn, "6 ways to keep employer data secure when working remotely," 2019. [Online]. Available: https://www.cmswire.com/information-management/6-ways-to-keep-employer-data-secure-when-working-remotely/

[26] J. Anderson, "Experts say the 'New Normal' in 2025 will be far more tech-driven, presenting more big challenges," 2021. [Online]. Available: https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges/

[27] N. Cory, "Cross-border data flows: Where are the barriers, and what do they cost?," 2017. [Online]. Available:

https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

[28] J. Gervais, "What is a VPN?," 2021. [Online]. Available: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

[29] J. Jang-Jaccard, and S. Nepal, "A survey of emerging threats in cyber security," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973-993, ISSN 0022-0000, 2014. [Online]. Available: https://doi.org/10.1016/j.jcss.2014.02.005. https://www.sciencedirect.com/science/article/pii/S0022000014000178

[30] D. Gewirtz, "What is a VPN and why do you need one? Everything you need to know," 2021. [Online]. Available: https://www.zdnet.com/article/what-is-a-vpn-and-how-does-it-work/

[31] S. Beaver, "10 top financial challenges for small businesses and how to overcome them," 2020. [Online]. Available: https://www.netsuite.com/portal/resource/articles/business-strategy/small-business-financial-challenges.shtml