International and Comparative
Corporate Law Journal
ISSN: 1388-7084 & E- ISSN: 1875-8290

Emerging Threats In Online Retail And How To Protect Them

Sebastian Clarke
Meridian Governance Initiative, Wellington, New Zealand

Received: 22/10/2025 **Accepted:** 17/02/2026 **Published:** 15/05/2026

Abstract
Technology and customer behaviour are driving e-commerce growth, making it more exposed to cybersecurity risks. This article analyses present and potential cybersecurity threats to online merchants and customers in e-commerce. We examine how data breaches, phishing schemes, ransomware attacks, and supply chain vulnerabilities affect the e-commerce sector using current research and industry reports. This paper also examines how cybercriminals are becoming more sophisticated, cloud computing and mobile technologies are expanding the attack surface, and data-driven business models are increasing cybersecurity threats in e-commerce. Businesses may defend their e-commerce operations and client data by understanding cybersecurity threats' basic causes and dynamics.
Keywords : Data breaches, cybersecurity, online shopping, dangers, current trends, ways to lessen their impact

Introduction

With its ever-increasing popularity, online shopping has changed the game for both companies and customers by making a previously inaccessible market more accessible, convenient, and personalised. While internet shopping has revolutionised the industry, it has also introduced new risks, the most significant of which is the constant risk of cyberattacks. Data breaches, identity theft, financial fraud, and supply chain disruptions are just some of the cyberattack dangers that have been connected with the increasing complexity and volume of online transactions. an in-depth analysis of cyber risks to online business, uncovering critical patterns, weak spots, and countermeasures to these ever-changing dangers. Our goal in exploring the complexities of cybercrime in the e-commerce ecosystem is to illuminate the complex issues that online merchants, customers, and other players face.

The Rise of E-Commerce: Opportunities and Challenges

With the rise of the internet and other digital technologies, companies are able to transact business more easily regardless of their location or the time zone difference. With e-commerce platforms, companies have access to global markets like never before, and consumers have the convenience of purchasing and transacting online at their fingertips. In today's digital age, companies of all sizes rely on e-commerce platforms to connect with consumers, generate sales, and increase their market share. Cybercriminals are always looking for new ways to exploit weaknesses in digital infrastructure and prey on unsuspecting victims for financial benefit; unfortunately, the fast growth of e-commerce has also put companies and customers at risk of a multitude of cybersecurity risks. There is a growing concern about the security and privacy of online transactions due to the prevalence and sophistication of cyberattacks, which include social engineering strategies as well as more traditional hacking approaches.

Understanding Cybersecurity Threats in E-Commerce

When it comes to online transactions, cybersecurity risks may take many forms, all with the same goal: to jeopardise the privacy, availability, and integrity of sensitive information stored in digital databases. Common dangers include data breaches, in which sensitive information like payment details and customer credentials is stolen or leaked; phishing scams, in which users are tricked into divulging personal information through deceptive emails or websites; ransomware attacks, in which data is encrypted and demands payment to decrypt it; and supply chain vulnerabilities, in which e-commerce systems are accessed unauthorizedly by exploiting weaknesses in third-party vendors and service providers.

The Need for Effective Mitigation Strategies

Online transactions and sensitive information must be protected by effective mitigation measures due to the ubiquitous nature of cybersecurity risks in e-commerce. Implementing strong security protocols, utilising advanced threat detection and response technologies, raising employee awareness and training, and forming partnerships with other businesses, government agencies, and cybersecurity professionals are all parts of these multi-layered strategies.

What follows is an examination of the most pressing cybersecurity concerns confronting online retailers, a survey of current trends in cybercrime, and some suggestions for reducing such dangers. Businesses can increase consumer trust and confidence, fortify their defences against cyberattacks, and guarantee the continued success of e-commerce as a secure platform for

online transactions by learning about the dynamics of cyber threats and implementing proactive security measures.

The Growth of E-Commerce

With the rise of e-commerce, which disrupts conventional business models, the purchasing and selling of products and services has undergone a sea change in the last few decades. Buying and selling products and services using the internet is known as e-commerce, or electronic commerce. What started out as a cool experiment in the early days of the Internet has turned into a worldwide phenomenon, changing the way people shop and causing the economy to grow at an unprecedented rate.

The First Stages: When companies started playing around with EDI systems in the 1970s and 1980s, they were essentially laying the groundwork for what is now known as electronic commerce. The advent of the internet and more user-friendly browsers in the 1990s, however, were major factors in the explosive growth of online shopping.

A time of fast expansion and investment in companies based on the internet, known as the dot-com boom, began in the late 1990s. The likes of Yahoo!, Amazon, and eBay rose to prominence as trailblazers in innovative business practices that shook up established markets. There was a mad dash of investment and invention caused by the allure of online shopping, which could connect people all over the world and make transactions easier.

Adoption by the Masses: As more people acquired internet connection and became used to buying things online, e-commerce went from being a niche business to being a phenomenon in the early 2000s. Technology advancements, like improved internet connectivity and safer payment methods, have contributed to the explosion of online shopping. More recently, the proliferation of mobile devices has further sped up the expansion of online shopping, allowing customers to shop whenever and wherever they like, right from their fingertips. An increasing percentage of all online purchases are now being processed using mobile devices, a phenomenon known as m-commerce.

The Effect on a Global Scale: Nowadays, online shopping connects people all over the globe, regardless of their location or cultural background. Because of the ease with which companies may now contact clients in faraway parts of the world, e-commerce has created new possibilities and markets for companies of all sizes.

Looking Ahead: With ongoing innovation and technical progress set to further transform the sector, the future of e-commerce seems promising. The next wave of e-commerce

advancements, including AI, VR, blockchain, and cryptocurrency, is going to change the game in ways we can't even begin to fathom.

Cybersecurity Risks and Their Effects on Online Shopping

Businesses and customers have reaped many advantages from e-commerce's meteoric rise, but there are also several cybersecurity risks that have the potential to severely impact online transactions and operations. Cybersecurity risks to e-commerce may cause extensive and serious harm, including data breaches, financial fraud, interruptions to the supply chain, and damage to reputation.

Financial Losses: Loss of funds is one of the most noticeable and direct effects of cyber risks on online shopping. In instance, valuable consumer data like credit card numbers and personal identifying information may be stolen in data breaches and then sold on the dark web or used for fraudulent purposes. As if the loss of income and harm to the brand's image weren't bad enough, the expense of remediation might include regulatory penalties, compensation to impacted parties, and legal expenses.

Cybersecurity events have the potential to damage consumer trust and confidence in online marketplaces, which in turn may cause a decrease in sales and the loss of consumers. Customers may look for other channels or stores to shop at if they are concerned about the security of their personal information while they shop online. Transparency, accountability, and measurable improvements to security measures are necessary to begin the long and difficult process of rebuilding trust and restoring confidence after a cybersecurity compromise.

Website unavailability, service interruptions, supply chain delays, and logistical issues are just a few ways in which cybersecurity risks may wreak havoc on e-commerce companies. For instance, e-commerce websites may become unavailable to consumers and the flow of online transactions may be interrupted if servers and infrastructure are overwhelmed by distributed denial-of-service (DDoS) assaults. Ransomware attacks that target e-commerce platforms or third-party suppliers may also cause delays in order fulfilment and delivery by disrupting supply chains.

Cybersecurity events in e-commerce may lead to legal and regulatory complications. Companies may be subject to inspections, fines, and lawsuits if they are found to be not in compliance with data protection laws and regulations. Businesses are now subject to more stringent requirements regarding the collection, storage, and use of customer data as a result of data privacy regulations passed by governments worldwide. These regulations include the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy

Act (CCPA) in the US. Serious penalties and harm to one's credibility may ensue from disobeying these rules.

The most sinister effect of cyber attacks on online trade is the harm they may do to companies' reputations over the long run. Brand equity and consumer loyalty may take a serious hit if a high-profile data breach or security event damages a company's image and erodes consumer trust. Consumers whose confidence a firm lost due to a data breach or who see the firm as careless in protecting their personal information may be difficult to win back, even after the firm has taken corrective actions and improved its security.

Conclusion

Due to the incredible accessibility, variety, and ease offered by the online marketplace, the meteoric rise of e-commerce has revolutionised the way companies function and customers purchase. Nevertheless, the constant risk of cybersecurity breaches is one of the new difficulties that have emerged as a result of this shift. Cybercriminals' plans and tactics are always evolving with e-commerce, so it's crucial for companies to take proactive measures to reduce cybersecurity risks and safeguard online transactions. Threats to e-commerce cybersecurity are ever-changing because cybercriminals are becoming smarter about the strategies they use to get into networks and steal data. There is a wide variety of serious and varied dangers that e-commerce companies face today, including data breaches, financial fraud, ransomware, and supply chain vulnerabilities. Cybercriminals face new threats and possibilities brought about by new trends, such as the expansion of mobile commerce, the number of IoT devices, and the development of more sophisticated AI.The future of online store security is fraught with peril and opportunity. Businesses must keep their guard up and be proactive in their fight against cyberattacks since cyber threats are always changing and multiplying. New possibilities for improving cybersecurity and reducing risks in the online marketplace are presented by technological developments like quantum computing, machine learning, and blockchain. Businesses can succeed in the ever-changing cybersecurity world by keeping up with the latest trends and best practices. Cybersecurity risks in online shopping pose a serious problem for companies and customers, but they also provide a chance to work together and come up with new solutions. Businesses can make e-commerce a safer and more reliable platform for online transactions in the long run, increase consumer trust and confidence, and reduce financial and reputational risks by taking a proactive approach to cybersecurity and implementing strong mitigation strategies.

References

1. Cisco. (2020). *Cisco 2020 Cybersecurity Report*. Retrieved from https://www.cisco.com/c/en/us/products/security/security-reports.html
2. Europol. (2020). *Internet Organised Crime Threat Assessment (IOCTA) 2020*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020
3. Kaspersky. (2021). *Kaspersky Security Bulletin 2020*. Retrieved from https://www.kaspersky.com/blog/kaspersky-security-bulletin-2020-key-figures-and-statistics/
4. McAfee. (2020). *McAfee Threats Report: Fourth Quarter 2020*. Retrieved from https://www.mcafee.com/enterprise/en-us/threat-center/threat-report.html
5. Ponemon Institute. (2020). *Cost of a Data Breach Report 2020*. Retrieved from https://www.ibm.com/security/data-breach
6. Symantec. (2020). *Internet Security Threat Report Volume 25*. Retrieved from https://www.broadcom.com/company/newsroom/press-releases/2020/symantec-2020-internet-security-threat-report
7. Verizon. (2020). *Verizon Data Breach Investigations Report 2020*. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/
8. World Economic Forum. (2020). *Global Risks Report 2020*. Retrieved from https://www.weforum.org/reports/the-global-risks-report-2020/
9. Yoo, Y., & Ha, T. (2020). Cybersecurity Risk and E-Commerce Performance: A Moderated Mediation Model. *Journal of Management Information Systems, 37*(1), 179-212. doi:10.1080/07421222.2020.1719935
10. Zhang, S., & D'Arcy, J. (2020). Supply Chain Cybersecurity: Challenges and Solutions for E-Commerce. *Information Systems Frontiers, 22*(5), 1079-1093. doi:10.1007/s10796-020-10056-5