INTERNATIONAL CONFERENCE ON RESEARCHES IN ENGINEERING, SCIENCE, TECHNOLOGY, MANAGEMENT AND HUMANITIES (ICRESTMH – 2024)

25TH AUGUST, 2024

CERTIFICATE NO : ICRESTMH /2024/C0824829

Impacts of Cybercrime on E-Commerce Businesses

Amshala Shankaraiah

Research Scholar, Ph. D. in Law, P.K. University, Shivpuri, M.P., India.

ABSTRACT

Cybercrime significantly impacts e-commerce businesses, posing threats to their financial health, reputation, and customer trust. Cybercriminals employ tactics like phishing, data breaches, ransomware, and identity theft, targeting sensitive customer information such as credit card details and personal data. These attacks can lead to substantial financial losses, both directly through stolen funds and indirectly through penalties for non-compliance with data protection regulations. When an e-commerce business experiences a security breach, the damage to its reputation can be severe. Customers often lose trust in platforms unable to protect their data, leading to a drop in sales and customer retention rates. Additionally, businesses may need to invest heavily in cybersecurity measures, increasing operational costs. The impact extends beyond financial aspects, as the threat of cybercrime also undermines the stability of the entire e-commerce ecosystem. Small and medium-sized enterprises (SMEs) are particularly vulnerable, as they may lack the resources for robust cybersecurity defenses. Legal liabilities and potential lawsuits further strain affected businesses. To combat these challenges, e-commerce companies must adopt proactive measures, such as encryption, multi-factor authentication, and regular security audits. Enhancing consumer awareness about safe online practices is equally important to foster a secure online shopping environment, thereby mitigating the impacts of cybercrime.