Page 3641 - 3651

DOI: *https://doij.org/10.10000/IJLMH.119442*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

E-Commerce and its Threat to Cyber-Security: The Legal and the Technological Aspect

ANANYA MITTAL[1]

ABSTRACT

E-commerce has emerged as a pivotal pressure in transforming international alternate, providing unmatched comfort and accessibility to consumers and businesses alike. but, this digital evolution has include a parallel upward push in cybersecurity threats, posing huge prison and technical demanding situations. This research paper explores the intersection among e-trade and cybersecurity, studying the widespread cyber threats targeting virtual commerce systems and comparing the effectiveness of cutting-edge felony frameworks designed to cope with those threats.

The look at cybersecurity describes the most prominent cybersecurity threats—phishing, square injection, ransomware, denial-of-provider attacks, and payment fraud—and examines how vulnerabilities in e-commerce systems reveal customers to monetary and identification theft. thru designated case research inclusive of the goal (2013), eBay (2014), and Equifax (2017) breaches, the paper highlights systemic safety lapses, the function of company negligence, and the restrictions of current enforcement protocols.

The paper critically assesses main regulatory devices, together with the overall statistics safety regulation (GDPR) of the eu Union, the California client privateness Act (CCPA), and India's facts era Act, 2000 and the proposed private facts safety invoice (PDPB). even though those frameworks goal to enhance digital security and records safety, enforcement inconsistencies, jurisdictional overlaps, and compliance challenges appreciably avert their effectiveness. pass-border e-commerce pastime further complicates criminal accountability and regulatory cooperation, as cybercriminals take advantage of gaps in global jurisdiction and divergent statistics protection requirements.

In its concluding segment, the paper proposes complete techniques for reinforcing e-trade cybersecurity. suggestions encompass the harmonization of world cybersecurity legal guidelines through worldwide treaties, the combination of AI-driven fraud detection systems, and the release of public attention initiatives to bolster customer cyber hygiene. The want for a balanced legal method that protects privateness at the same time as allowing effective cyber defense is emphasised.

[1] Author is a student at Christ University, Delhi Ncr, India.

I. Introduction

E-commerce has revolutionized global trade and the behaviour of consumers. The shift to digital has made these transactions easier and more accessible, leading to massive growth in the space. As digital markets continue to develop, global e-commerce sales reached $26.7 trillion in 2021, according to the United Nations Conference on Trade and Development (UNCTAD), and this number has remained steadily increasing.[2] With that growth, though, has come a troubling rise in the cybersecurity threat landscape. Cybercriminals take advantage of technology vulnerabilities, weak regulatory oversight, and cross-border jurisdictional conflicts to mount sophisticated attacks against consumers and companies.

Legal frameworks like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) try to enforce data security in online transactions, but their enforcement is patchy, and existing measures seldom deter cybercriminals. Among them are phishing and identity theft, as well as mass-scale ransomware attacks that paralyze companies. In this paper, we will study the major threats that ecommerce merchants face in terms of cybersecurity, go over the most important laws and regulation regarding data security and finally analyse whether the current framework is suited to combat such threats.

The study is organized in five stages. The first part describes the most common cybersecurity threats for e-commerce. The second looks at large case studies that illuminate weaknesses in existing security systems. In the third section, we review the existing global legal regimes for e-commerce security. The fourth examines the legal and enforcement challenges complicating cybersecurity governance, and the final section provides policy recommendations designed to bolster cybersecurity efforts.

II. The major cybersecurity threats in e-commerce

E-commerce platforms hold huge troves of sensitive customer data, including financial information, personal identifiers, and shopping histories. As transactions become more digitalized, these platforms are becoming the ultimate data transfer target for cybercriminals, who use sophisticated mechanisms to exploit holes in security-based systems.

Phishing and Social Engineering

Phishing attacks are one of the most simplistic and effective cyber threats in e-commerce. Cybercriminals pretend to be valid businesses, resulting in phishing emails, text messages, or

[2] "United Nations Conference on Trade & Development, *Global E-Commerce Growth*, U.N. Doc. UNCTAD/DTL/STICT/2021 (2021), https://unctad.org/news/global-e-commerce-sales-jump-267-trillion-covid-19-boost."

scam websites tricking users into submitting their sensitive credential data.[3] Based on research from the Anti-Phishing Working Group (APWG), phishing against online payment service providers climbed 48% last year where e-commerce platforms were top targets.[4]

Common examples include things like the Amazon phishing scam, where hackers send emails informing users of problems with their customer accounts and directing them to log in on a fake website. Worse, all that stolen data is then used to commit identity theft, make unauthorized transactions, and attempt more phishing.[5] Cross-border phishing scams still thrive around regulatory loopholes even under strict regulations like GDPR.

SQL injection & Cross-site scripting (XSS)

SQL injection – The Most Significant E-Commerce Attack Vector Structured Query Language (SQL) injection and Cross-Site Scripting (XSS) are two of the most common types of attack vectors used against e-commerce. SQL injection attacks happen when hackers can exploit weaknesses in databases integrated with web applications — allowing them to alter database queries, extract sensitive information, etc.[6]

A XSS vulnerability was responsible for the breach of 380,000 customer transactions from British Airways back in 2018. Hackers injected malicious code into the airline's website that redirected users to a fake payment page, from which their credentials were harvested.[7] Other such cases include: (2014) Alibaba — 20 million user accounts compromised — which further emphasizes the urgency of ensuring double encryption input validation on web servers.

Ransomware and Malware Attacks

Ransomware attacks are one of the main causes of financial and operational disruption in e-commerce. Ransomware that encrypts vital business information, making it impossible to access until a ransom is paid.[8] While the 2021 Colonial Pipeline ransomware attack was aimed not at e-commerce but rather at an infrastructure, it showed the crippling impacts of a successful

[3] "National Cyber Security Centre, *Understanding Social Engineering Attacks*, NCSC (2022), https://www.ncsc.gov.uk/guidance/phishing-attacks."

[4] "Anti-Phishing Working Group, *Phishing Activity Trends Report: 2022*, APWG (2022), https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf."

[5] "Amazon Customer Service, *Recognizing and Avoiding Phishing Emails*, Amazon (2022), https://www.amazon.com/gp/help/customer/display.html?nodeId=GKVJJQ8FA46DB8S3."

[6] "Open Web Application Security Project, *SQL Injection: Prevention Guide*, OWASP (2021), https://owasp.org/www-community/attacks/SQL_Injection. "

[7] " U.K. Information Commissioner's Office, *British Airways Data Breach Fine*, ICO Enforcement Report (2020), https://ico.org.uk/action-weve-taken/enforcement/british-airways "

[8] "Federal Bureau of Investigation, *Ransomware: An Increasing Threat to Businesses*, FBI Cyber Division Bulletin (2021), https://www.ic3.gov/Media/Y2021/PSA210505."

attack, forcing fuel distribution across the United States to be brought to a halt.[9]

Global ransomware damages are projected to cost victim businesses more than $265 billion per year by 2031, according to Cybersecurity Ventures, and e-commerce businesses are a prime target given their heavy reliance on digital infrastructure.[10] Moreover, while cybersecurity laws explicitly penalize the dissemination of ransomware, anonymous payment mechanisms such as cryptocurrency make it difficult for authorities to pursue cases.

Denial of Service (DoS) Attacks

Denial-of-Service (DoS) attack: In a DoS attack, the e-commerce website's servers are overwhelmed with data from multiple sources, which effectively stops the process of the site, making it inaccessible to legitimate users. Attackers use DDoS attacks by generating excessive traffic using botnets.[11]

DDoS attacks against online storefronts rose by 150%, according to a 2021 Akamai Technologies report, especially during the busiest shopping seasons, such as Black Friday and Cyber Monday.[12] E-commerce behemoths like Amazon and Shopify shell out big bucks for DDoS mitigation tech, but smaller businesses are left vulnerable.[13]

Fraudulent Payments and Identity Theft

The rise in digital transactions has made payment fraud a serious concern for e-commerce platforms. Credit card frauds are carried on by cybercriminals by mishandling stolen credit card details, synthetic identities, and through automated bots.[14]

Data from a 2022 report published by CyberSource, a subsidiary of the multi-national Visa payment technology company, indicates that more than $20 billion in costs globally were associated with e-commerce fraud, with small and medium-sized businesses generating the most collateral damage.[15] Although there are standards in place in the industries, such as PCI-DSS (Payment Card Industry Data Security Standard), most online merchants do not have

[9] Id.

[10] "Cybersecurity Ventures, *The Ransomware Economy* (2022)."

[11] "U.S. Department of Homeland Security, *Denial-of-Service Attacks: Trends and Prevention Strategies*, DHS Cybersecurity & Infrastructure Security Agency Report (2021), https://www.cisa.gov/sites/default/files/publications/DDoS_Fact_Sheet_508C.pdf."

[12] "Akamai Technologies, *State of the Internet: E-Commerce Cybersecurity Report*, Akamai Threat Intelligence (2021), https://www.akamai.com/site/en/documents/state-of-the-internet/q4-2021-soti-security-report.pdf.

[13] "Shopify Security Team, *DDoS Protection Strategies for E-Commerce Businesses,* Shopify White Paper (2022), https://www.shopify.com/enterprise/ddos-attack-prevention. "

[14] "Financial Action Task Force, *Payment Fraud and E-Commerce Crime Trends*, FATF Report (2021), https://www.fatf-gafi.org/en/publications/methodsandtrends/payment-fraud.html."

[15] "CyberSource, *2022 Global E-Commerce Fraud Report*, Visa Cybersecurity Division (2022), https://www.cybersource.com/content/dam/documents/global-fraud-report-2022.pdf."

proper fraud detection systems set in place.[16]

III. E-COMMERCE CYBERSECURITY BREACHES: CASE STUDIES

E-commerce platforms, which store large amounts of sensitive data, have long been readily attacked by hackers. High-profile breaches expose not only millions of users to fraud but also reveal regulatory weaknesses and corporate lapses on security. Here are some of the largest e-commerce breaches to date.

Target Data Breach (2013)

The Target data breach of 2013 is still one of the largest data breaches in retail history, exposing more than 40 million credit and debit card records.[17] Cybercriminals took advantage of poor security protocols in Target's third-party vendor system to access its payment network and extract customer data. In 2017, Target agreed to a $18.5 million settlement of a multi-state lawsuit involving 47 U.S. states about its failure to protect customer data.[18] The breach spurred class-action lawsuits, which caused Target to pay $10 million in damages to consumers affected.[19] As this article shows, they even faced federal investigations over its compliance with Payment Card Industry Data Security Standard (PCI-DSS) and ended up costing the company a total of $202 million.[20]

This case highlighted the need for strong vendor security policies and tighter regulatory scrutiny of third-party access to payment systems.

eBay Data Breach (2014)

In 2014, hackers breached eBay's corporate network, and along the way, stole 145 million user accounts, including names, email addresses, encrypted passwords and phone numbers. The attackers gained undeterred access to eBay's internal systems, tunnelling in via stolen employee credentials. At the time, GDPR was not in effect, but regulators later pointed to eBay's lack of response as an example of why stronger data protection laws were needed. That caused a major hit to eBay's reputation, and trust and active users started to drop. To prevent this kind of unintentional data breach, companies should focus on multi-factor authentication

[16] "Payment Card Industry Security Standards Council, *PCI-DSS Compliance Guide*, PCI Security Standard v4.0 (2022), https://www.pcisecuritystandards.org/documents/PCI_DSS_v4-0.pdf."

[17] "*In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154 (D. Minn. 2014)."

[18] "Fed. Trade Comm'n, *Target Settles Data Breach Lawsuit*, FTC Enforcement Report (2017), https://www.ftc.gov/news-events/press-releases/2017/05/target-settles-breach-case."

[19] Id.

[20] " Payment Card Indus. Sec. Standards Council, *PCI-DSS Compliance Guide*, PCI Sec. Standard v4.0 (2022), https://www.pcisecuritystandards.org/documents/PCI_DSS_v4-0.pdf. "

and employee cybersecurity best practices.[21]

Equifax Data Breach (2017)

Equifax Breach (2017) Although this breach isn't directly related to e-commerce, it remains one of the most damaging cybersecurity breaches in history, exposing 147 million individuals' financial data.[22] The breach originated from unpatched vulnerabilities in Equifax's Apache Struts software, which granted attackers months of unauthorized access. Equifax agreed to pay $700 million to the U.S. Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and state agencies.[23] The data breach led to regulatory scrutiny worldwide and formed the basis for GDPR implementation mechanisms in the EU. This case illustrates corporate misconduct regarding the timely update of security patches, highlighting the legal obligation to update software in a prompt manner and maintain adherence to cybersecurity frameworks.

(A) Legal Frameworks Governing Cybersecurity in E-Commerce

Cyberattacks are becoming more and more common with e-commerce security regulations fragmented. Standards of practices like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) aim to align cybersecurity practices globally but they continue to struggle with enforcement issues.

GDPR – General Data Protection Regulation – European Union

The GDPR, adopted in 2018, is the world's most expansive data protection law, placing stringent security requirements on businesses that work with personal data of residents in the European Union.[24]

- Article 32 requires businesses to use "appropriate technical and organizational measures" to secure user data.
- Article 33 mandates that companies notify of data breaches within 72 hours.
- Penalties: Failure to comply can result in penalties of up to €20 million or 4% of global revenue.

The GDPR has significantly impacted global e-commerce platforms, compelling companies

[21] "Tom Warren, *eBay Confirms 145M User Data Breach*, The Verge (May 21, 2014), https://www.theverge.com/2014/5/21/5739154/ebay-data-breach-user-details-stolen. "

[22] *In re Equifax Inc. Sec. Breach Litig.*, 362 F. Supp. 3d 1295 (N.D. Ga. 2019).

[23] U.S. Fed. Trade Comm'n, *Equifax Settles Data Breach for $700 Million*, FTC Report (2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-data-breach-settlement.

[24] Gen. Data Protection Reg. (EU) 2016/679.

such as Amazon, Alibaba, and eBay to revise their data security policies. Many businesses have incorporated Privacy by Design principles, ensuring that cybersecurity considerations are embedded in every stage of product and service development.[25]

California Consumer Privacy Act (CCPA) – US

The CCPA, enacted in 2020, is the most robust privacy law in the United States, giving California residents more power over their data.[26] Under this, consumers have the right to request deletion of or disclosure about the personal information that businesses have collected about them. It also requires companies to offer the ability to opt out of sales of their data. Fines are from $2,500 per unintentional violation to $7,500 for wilful violations. However, it must be highlighted that the differences in cybersecurity policy at a state level create inconsistencies in national security. The CCPA also does not enforce strong breach notification requirements like GDPR, making it less effective against cybercrime.[27]

Information Technology Act, 2000 & Personal Data Protection Bill, India

The key technology legislation in India is the Information Technology Act, 2000,[28] and the Personal Data Protection Bill (PDPB)[29] is aimed at providing GDPR-like protections. Section 43A of the IT Act imposes liability on entities that fail to protect sensitive personal data, requiring them to compensate affected individuals. The PDPB (Upcoming) introduces data localization requirements, mandating that critical personal data of Indian citizens be stored within the country. This provision presents significant challenges for global e-commerce platforms reliant on cross-border data transfers.

(B) Legal Challenges in Cybersecurity for E-Commerce

In spite of global cybersecurity standards, the melding of data protection law with e-commerce is an uneven and unpredictable process. There are now several legal and regulatory hurdles that make putting strong cybersecurity standards in place in the online marketplace complicated.

These challenges with cross-border jurisdiction and enforcement

E-commerce platforms can transcend borders, but cybersecurity regulations are jurisdictionally limited, leaving gaps in enforcement. An example of this is an e-commerce platform in the U.S.

[25] "David Meyer, *How GDPR Forced Amazon, eBay, and Other Retail Giants to Rethink Data Security*, Fortune (May 24, 2019), https://fortune.com/2019/05/24/gdpr-amazon-ebay-data-privacy/. "

[26] Cal. Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 (West 2020).

[27] "Caitlin Fennessy, *How U.S. Privacy Laws Compare to GDPR: CCPA's Shortcomings*, Int'l Ass'n of Privacy Profs. (IAPP) (2020), https://iapp.org/news/a/ccpa-vs-gdpr-comparing-u-s-state-privacy-laws-to-eu-regulations/. "

[28] The Information Technology Act, No. 21 of 2000, § 43A, Acts of Parliament, 2000 (India).

[29] Personal Data Protection Bill, No. 373 of 2019, § 33, Acts of Parliament, 2019 (India).

that services European customers must comply with GDPR, as well as domestic U.S. regulations. This overlap of regulatory jurisdiction complicates compliance, while allowing cybercriminals to take advantage of jurisdictions with lax cybersecurity laws to operate.

A prominent recent example is that of Facebook v. Ireland's Data Protection Commission (2020), in which the European Court of Justice (ECJ) ruled that companies in the U.S. that process data about EU citizens must guarantee compliance with GDPR, functionally "blocking" the U.S.-EU Privacy Shield framework.[30] This decision highlights the legal tensions of cross-border furor around enforcement in e-commerce cybersecurity.

Variability in Regulatory Enforcement and Compliance Difficulties

While robust cybersecurity mandates are enshrined in data protection laws like GDPR and CCPA, these laws are not uniformly enforced across regions. The e-commerce platforms are rarely closely monitored by regulatory bodies appearing unable to keep close watch, which often results in avoiding the penalties for a lot of non-compliance companies.[31]

However, even thought the GREENPEACE has to report other companies that notice a data breach within 72 hours because of the GDPR, many of them hide it because of the bad image and the financial problems they could encounter.[32] A 2022 DLA Piper study indicated that more than 60 percent of companies subject to GDPR violations have not reported data breaches in the time required by law.[33] This demonstrates how difficult it is to enforce compliance with cybersecurity standards — even with the world's most comprehensive data protection legislation in place.

Reconciling Cybersecurity with Privacy Rights

One major legal issue in the field of cybersecurity is the conflict between the necessity to implement security solutions and the right to privacy of the individual. Stricter cybersecurity policies frequently introduce increased data monitoring, behavioural tracking, or biometric authentication that can be at odds with user privacy laws.[34]

One of the most notable examples is the, so-called, Apple v. FBI case, (2016) in which the FBI sought a court order ordering Apple to unlock an encrypted iPhone belonging to a terrorist. Apple declined, arguing that doing so would violate users' right to privacy, setting off a wider

[30] Case C-311/18, *Facebook Ireland Ltd. v. Data Protection Comm'r*, 2020 E.C.R. I-1226.
[31] "Paul Schwartz, *The Gap in Data Protection Enforcement: GDPR vs. CCPA*, 48 Harv. J.L. & Pub. Pol'y 97 (2021), https://harvardlawreview.org/data-enforcement-gap. "
[32] "Gen. Data Protection Reg. (EU) 2016/679, art. 33."
[33] "DLA Piper, GDPR Fines: Global Trends and Enforcement Reports 2022, DLA Piper Privacy Group (2022), https://www.dlapiper.com/gdpr-fines-report-2022.pdf."
[34] Id.

debate over whether companies should be legally required to give the government access to user data when law enforcement officials say it is needed for security reasons.[35]

E-commerce companies have the same issues:

More robust fraud detection mechanisms (biometric verification, AI-powered tracking, etc.) frequently are associated with massive consumer data collection, and therefore invoke privacy concerns. GDPR and CCPA compel platforms to enable users to opt out of data scraping activity, consequently breaking those security shields against fraud and cyberattacks. The latest clash illustrates the importance of not overcorrecting in favour of consumer privacy at the expense of practical cybersecurity protections.

New Threats and Legal Loopholes

The growth of AI-driven cyberattacks and cryptocurrency-based fraud creates new legal challenges that falls outside the scope of existing cybersecurity laws.[36] Phishing attacks powered by AI: Cybercriminals are using deepfake technology and AI-generated phishing emails to thwart traditional fraud detection methods. No laws currently comprehensively regulate AI-based cyber threats.

Cryptocurrency and money-laundering: As laws stand, most ransom attacks are paid in cryptocurrency, which makes tracking illegal transactions nearly impossible for law enforcement.[37] The absence of international cryptocurrency regulation allows cybercriminals to avoid prosecution. These newfound threats reveal regulatory weaknesses in e-commerce cyber and call for updating legal frameworks to tackle emerging cyber threats.

(C) Best Practices to Strengthen Cybersecurity in E-Commerce

As companies face increasing cybersecurity threats to e-commerce, legal and technical efforts to improve data protection, regulatory compliance, and cross-border enforcement will likely be needed.

Global Harmonization of Cybersecurity Regulations

Harmonising cybersecurity laws across the globe will certainly be needed when several jurisdictions are involved. A UN-backed cybersecurity treaty, akin to the Budapest Convention on Cybercrime, could offer a standardized legal framework for global collaboration.[38]

[35] "*Apple Inc. v. FBI*, 137 S. Ct. 2197 (2016)."

[36] "Europol, *AI and Cybercrime: The Rising Threat of Automated Attacks*, Europol Cybercrime Div. (2023), https://www.europol.europa.eu/ai-cybercrime-threat."

[37] "Fin. Action Task Force, *Cryptocurrency-Based Money Laundering in Cybercrime*, FATF Report (2022), https://www.fatf-gafi.org/publications/cryptocurrency-money-laundering."

[38] "Council of Europe, *The Budapest Convention on Cybercrime*, COE Treaty Series No. 185 (2001)."

Data security obligations should be standardized across the board, with GDPR-like regulations expanded globally. These mutual legal assistance agreements (MLATs) should allow for greater cross-border enforcement of cybersecurity.

Improving Consumer Awareness and Cybersecurity Education

April 30, 2023 in Cybersecurity Consumer awareness: A key but often overlooked element of cybersecurity A lot of phishing and fraud attacks work simply because users do not know. Governments should initiate cybersecurity awareness campaigns to ensure that consumers understand how to engage safely in e-commerce.[39] AI-powered fraud detection tools can help e-commerce platforms fend off phishing scams and payment scams.[40]

AI Cybersecurity Solutions

With the emergence of AI-driven cyberattacks, AI should also be utilized for cyber defense systems. Real-time identification of fraudulent transactions using AI-based anomaly is done using an AI system. Authentication and verification will also ensure that only authorized individuals have access to the system, and the blockchain itself serves as a tamper-proof and immutable record of transactions.[41]

IV. Conclusion

Although e-commerce has revolutionized global trade, the rapid growth of e-commerce has also laid bare serious vulnerabilities in both cybersecurity and legal enforcement frameworks. Grabbing top position are phishing, ransomware, DoS attacks, and payment fraud, leveraging weaknesses in regulatory frameworks and enforcement gaps. Though laws such as the GDPR, CCPA and India's IT Act will attempt to normalize baseline security measures, the inconsistencies in enforcement, cross-border jurisdictional clashes and AI-enhanced cyber threats have created immense roadblocks.

To overcome these challenges, we need to harmonize international cybersecurity laws, strengthen regulatory enforcement, improve fraud detection through AI-based technology and raise consumer awareness. Evolving cyberthreats also require legal frameworks that balance security and privacy and hold e-commerce platforms accountable. In conclusion, a coordinated international response that optimally combines technological evolution and an enforceable legal

[39] "Nat'l Cyber Sec. Ctr., *Cybersecurity Awareness Guide for Consumers*, NCSC (2022), https://www.ncsc.gov.uk/cyber-awareness-guide. "

[40] "U.S. Fed. Trade Comm'n, *Cybersecurity Task Force: Strengthening E-Commerce Security*, FTC Report (2022), https://www.ftc.gov/cybersecurity-task-force-report. "

[41] "Blockchain Sec. Council, *How Blockchain Enhances E-Commerce Security*, BSC White Paper (2023), https://www.blockchainsecuritycouncil.org/blockchain-ecommerce.pdf. "

framework is essential to ensure the viability of the future digital marketplace in the face of ever-increasing cyber hackers.

*****