CYBERSECURITY ISSUES AND CHALLENGES IN E-COMMERCE

Snehal Bendrikar[*]

ABSTRACT

The advent of the digital age has resulted in a significant surge in e-commerce, which has been greatly enhanced by the synergistic relationship between technology, commerce, and customer involvement. First and foremost, though, there are obstacles: persistent increases in the likelihood of cyber threats are unmistakable barriers that undermine the integrity and the success of online business settings This study explores the implications of cyber threats to e-commerce, offers comprehensive solutions, and critically examines the compound enforcement of these risks. It is supported by prevalent risks, such as malware, spear phishing, data breaches, and payment fraud, all of which pose grave risks. The primary purpose of data breaches is to reveal the personal information of defenseless customers, cause financial losses, and negatively impact the opinions of those customers. In addition, spear phishing is a tactic that deceives recipients into disclosing critical information, jeopardizing users' privacy and undermining the legitimacy of systems. Transactions are directly hampered by payment scams, which include credit card data theft and chargeback scheme manipulation. In comparison, company equipment is rendered inoperable, and authentic customer databases are tainted by malware and ransomware. Cybersecurity battles involving e-commerce frameworks are especially difficult. They involve complex interwoven service chains and external collaborations, but they also include human weaknesses such as incorrect user input and insider threats. In order to protect digital commerce, this essay focuses on how legislators, e-commerce merchants, and cyber-security professionals would have been subject to a proactive cybersecurity response. Additionally, the report suggests that cybersecurity legislation should evolve dynamically in light of airborne cyber threats and the growing e-commerce industry. Through this analysis, I hope to provide recommendations for improving the resilience of digital commerce ecosystems by keeping an eye on the always-evolving cybersecurity front. I also hope to explore the psychology of cyber threats and evolving technology in the process.

Keywords: Cyber Security Issues, E-commerce, Security.

[*] BBA LLB, FOURTH YEAR, NEW LAW COLLEGE, PUNE.

INTRODUCTION

Cybersecurity is becoming more than just a technical requirement for e-business; it is a critical component of customer trust and long-term economic viability in today's digital environment. By eliminating regional barriers and establishing a global market, the emergence of e-business has revolutionized the way businesses operate. Due to advancements in internet technology, e-commerce has substantially evolved from its inception in the late 20th century to the huge digital arenas that we all enjoy today. Cybercriminals target e-commerce platforms because they are growing rapidly and attract millions of customers every day. Online shopping is made more exposed to a range of cyber threats by its very convenience—personal information is stored, and payments are made easily—data breaches, identity theft, and fraudulent transactions are just the tip of the iceberg. The goal of this essay is to thoroughly dissect and comprehend the various layers of complex cybersecurity concerns that modern e-commerce faces in the era of electronic transactions[1]. All individuals must be ready to delve into the fascinating realm of contemporary cybersecurity threats that are plaguing the e-commerce industry. These threats pose a significant threat to businesses and individuals who ultimately fall victim to the aftermath of cyberattacks. Additionally, these risks of cyberattacks exploit the multitude of transactions that occur online and in physical stores. This essay will not hold back in demonstrating the elements of common cybersecurity challenges and providing solutions to protect the e-commerce community from the myriad attacks that are constantly emerging in cyberspace.

CONCEPTUAL FRAMEWORK

Cybersecurity issues are serious and present a threat to both customers and businesses in the e-commerce industry. These risks undermine confidence in digital commerce platforms in addition to compromising private information. Creating effective countermeasures involves an understanding of the characteristics, manifestations, and effects of these threats.

Data Breaches

Data breaches are a serious danger to the e-commerce industry because they allow unauthorized parties to obtain private information about consumers, including their financial

[1] Papakonstantinou 2022. Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?https://www.sciencedirect.com/science/article/pii/S0267364922000012

and personal details. In 2018, one of the biggest online shops had a data breach[2] that resulted in the compromising of millions of people's personal information. It is important to note that these breaches were common. The immediate financial losses resulting from such breaches, the subtle scale of subsequent identity frauds that may happen years after the breach has been fixed, and possible damage to the brand's reputation are just a few of the numerous direct financial repercussions of such breaches. Thus, businesses in the e-commerce industry need to protect enormous data repositories from increasingly sophisticated hackers operating on a global scale, all the while customers and business associates are being destroyed by identity theft due to a lack of adequate prevention measures.

Phishing Attacks

Scams involving e-commerce can be very devious, fooling victims into divulging private information like passwords and credit card details. Customers may receive an email, for instance, stating that they need to update their account information using a fake link from a reputable online retailer. As a result, the customer's funds and account security suffer instant harm, which encourages additional illegal activity. The consequences are severe for e-commerce businesses; they include undermining customers' trust in the platform and threatening legal action or government intervention. These attacks chip away at one of the fundamental security pillars supporting the achievement of the online economy, undermining the already fragile relationship between consumers and online companies.

Payment Fraud

E-commerce payment fraud can include anything from credit card, debit card, or online payment system fraud to hackers' possible diversion of funds through online transaction manipulation or a more straightforward method of hacking into accounts and transferring money around to get it to their accounts so they can withdraw and spend it. Credit card fraud is one of the most prevalent types of online payment fraud. This occurs when credit card details are taken and used by someone else to make fraudulent internet purchases. Payment fraud, sometimes known as "friendly fraud" or chargeback fraud, is all too common. In this kind of fraud, a consumer purchases a thing online returns it to their bank, and claims not to have made the transaction at all. They receive their money back and the product they

[2] Sarker 2020. Cybersecurity data science: https://www.sciencedirect.com/science/article/abs/pii/S0140366419311880

purchased remains. Payment fraud is known to have costs, such as the instant losses that merchants experience as a result of these actions and the higher operating expenses that result for the impacted businesses in enforcing stricter security measures and prudent mediation procedures. Unfortunately, payment fraud is not an isolated issue. It also contaminates limited company resources and makes companies rethink how they provide customer service and how they will identify fraud in the always-changing internet marketplace.

Malware and Ransomware

Given that they represent some of the most dangerous intrusions currently in existence, malware and ransomware demand more careful consideration. Both of them use extremely cunning techniques to sneak into a system that is compromised. Malware, for instance, is capable of stealing personal information and is also easily able to follow any desired e-activity[3]. On the other hand, the latter type of ransomware encrypts important information and offers to sell the digital key to the highest bidder—in this scenario, typically the compromised e-commerce company itself. The severity of the problem can be best understood by using the example of a well-known online business that was attacked by ransomware. Even though the well-liked online company was experiencing strong business, it was attacked by ransomware that engulfed the customer data warehouses and severely disrupted sales activities, forcing a multi-day outage. E-commerce would be well-served by taking protections against malware and ransomware since there is a strong likelihood that significant judgments for these malicious incidents will depend on the acts of both the attacker and the ransomed.

Underlying Factors

The sophisticated web of interlocking services and third-party connections that form the foundation of e-commerce platforms has become a major element in the proliferation of cybersecurity threats. Even though they play a crucial part in providing essential elements like payment gateways, CRMs, and other procedures that result in high operational efficiencies, system expansion forces several weaknesses to remain hidden behind closed doors: served as the points of interaction between order management software, banking

[3] Bae 2020. Ransomware detection using machine learning algorithms. Concurrency and Computation: https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.5422

systems, logistics apps for corporate resource planning, and e-commerce sales consoles. It ends up somewhere similar: Multiple points of assault and exposure. Because of integration, it is now far simpler for attackers.

The human dimension, an unknown risk, follows from the intricacy of technology. Human error in avoiding security measures, a customer falling for a phishing scam, an insider purposefully sabotaging the system—any of these scenarios might cause chaos. A common attack vector is produced by complex system architectures and human mistakes. To successfully lower risk, a comprehensive cybersecurity strategy that combines cutting-edge technological defenses with in-depth awareness training is required.

In summary, there are many different types of cybersecurity risks in the e-commerce industry. Each type of attack has a unique strategy and set of outcomes. Customers lose trust in the organization and it is subject to regulatory scrutiny when highly personal identifying and financial information is compromised due to data breaches. Phishing occurrences deceive people into committing self-violations, which results in loss of revenue and unauthorized access to security. In addition to causing financial harm, occupancy frauds interfere with the integrity of trade and directly affect e-commerce companies. Apart from disrupting the system, malware and ransomware also fail to maintain the integrity, availability, or objective of the specific information.

CASE STUDIES

To illustrate the practical importance of cybersecurity risks to online shopping. To offer insightful guidance on how to strengthen cybersecurity rules, each scenario describes the vulnerabilities exploited, the steps taken, and the knowledge gained.

Case Study- 1

One of the biggest retail hacks ever happened at Target, a major American retailer with fast-expanding online sales, during the 2013[4] holiday season. This hack demonstrated the vulnerability of contemporary retail systems as well as the growing importance of cybersecurity inside the sector.

[4] Al Tamer 2021. The advantages and limitations of e-commerce to both customers & businesses. BAU JournalCreative Sustainable Development, 2(2), p.6. https://digitalcommons.bau.edu.lb/csdjournal/vol2/iss2/6/

Overview of the Incident

Target's point-of-sale (POS) cash registers were compromised by cybercriminals who installed software on them to steal credit and debit card information from customers. Initially, they gained access to Target's network by stealing the login credentials of a third-party HVAC vendor that the company had assigned account and system access to perform network maintenance. The point of the breach revealed critical weaknesses in Target's security and segmentation, allowing cybercriminals to begin their year-long campaign of theft and slow-walking the removal of 110 million Target customers' financial and personal data.

Immediate Response

Target moved fast as soon as it learned about the hack. The business launched a thorough forensic investigation to ascertain the scope and mechanics of the breach, and it promptly notified the general public and law enforcement. Target strengthened its network security and offered free credit monitoring to all victims in an effort to lessen the immediate harm and regain the trust of customers. This involved removing the malware from the systems and patching the holes that the attacker had previously used to gain access.

Financial Impact

With almost $292 million in costs, the data breach placed an enormous financial burden on its victims. A portion of these expenses went toward paying for the investigation into the breach's immediate costs. Other expenses included the money given to harmed parties and extra cash used for maintaining and enhancing network security. Target suffered less evident financial losses in addition to these more visible expenses as a result of sharply lower sales and a decline in shareholder value that included the difficult-to-quantify costs of disgruntled consumers leaving the store and never coming back. The breach was found during the busiest time of year for shopping—the holidays—which only served to exacerbate its negative consequences as already anxious customers, already low on trust, began to buy elsewhere. An already troubled Target saw its profits erode, and it has been working for over three years to win back the confidence of investors and customers.

Lessons Learned

The corporation completely redesigned its corporate cybersecurity policy in response to the Target data leak. In order to better oversee the organization's cybersecurity efforts, Target appointed a new Chief Information Security Officer (CISO) after realizing that stronger leadership was required in this crucial area. This turnabout demonstrated Target's resolve to strengthen its defenses against similar violations in the future. Target made the decision to invest heavily in cutting-edge cybersecurity technology in the wake of the hack in order to ensure that it wouldn't occur again. They currently possess the best intrusion detection and encryption technologies available for purchase as a result. They altered the architecture of their network as well, making it impossible for hackers to go from one compromised server to the next.

Employee training initiatives were crucial, Target provided personnel with extensive instruction on understanding and adhering to cybersecurity protocol.[5] Target's training program was created to address the human aspect of cyber security by equipping staff members with the knowledge and abilities to recognize and address any security risks.

Target has expanded the depth of its collaboration with top cyber security experts and other retail industry peers, exchanging knowledge and best practices to strengthen both the industry as a whole and Target itself. This strategy followed a broader trend of group dedication and unity against a variety of swiftly changing dangers, which was particularly evident among cyber security organizations.

CONCLUSION

Cybersecurity in the retail industry is said to have taken a significant turn when Target became the victim of a large data breach. Retailers are now more aware than ever of the critical need to implement stringent security measures in order to safeguard client data, especially payment information, in light of the event. The attack additionally demonstrated the intricacy of the risks associated with cybercrime and the necessity of all-encompassing solutions that include staff, technology, and cross-industry cooperation. By strengthening its processes and increasing general shoppers' trust in the reliability of its systems, Target

[5] Peters 2021. Growth Hacking: Techniques, Disruptive Technology-How 40 Companies Made It BIG–Online Growth Hacker Marketing. http://dspace.vnbrims.org:13000/jspui/bitstream/123456789/4780/1/Growth%20Hack

established new benchmarks for a more secure base that merchants and their e-commerce partners could build upon.

Case Study -2

The well-known financial company Capital One, which gained notoriety for having a significant online banking presence, suffered an incredible data breach in July 2019[6]. Around 30% of all adults in Canada and the United States were impacted by this data breach, which also compromised over 140k Social Security numbers and tens of thousands of bank account information belonging to over 100k consumers in each country. This specific occurrence serves as a sobering reminder of the widespread, terrifying vulnerabilities that large-scale digital infrastructures are prone to, as well as the frequently irreversible consequences that come with their exploitation.

Background

Capital One is among the select few financial organizations that made the decision to recognize the digital transformation in the banking industry at an early stage. As a result, the corporation became one of the factors behind Finch thanks to its investment in Internet banking. However, when Capital One performed their banking operations on the recently established digital realty and cloud computing architecture, they were exposed to hazards due to their laser-like march into the digital realm.

Details of the Incident

The security breach, which included a straightforward web application firewall misconfiguration, was the product of an inside job. The former employee of Amazon was able to obtain unauthorized access to data kept on AWS servers by exploiting this vulnerability. The method yielded a wealth of valuable data, including social security numbers, names, residences, credit scores, and credit scores of Capital One clients. There are obvious consequences for such a breach.

[6] Neto 2021. A CASE STUDY OF THE CAPITAL ONE DATA BREACH: WHY DIDN'T COMPLIANCE REQUIREMENTS HELP PREVENT IT Journal of Information System Security, 17(1). https://www.jissec.org/Contents/V17/N1/V17N1-Neto-p49.pdf

Immediate Response

Capital One moved swiftly and forcefully as soon as they discovered the breach. So that no more illegal individuals could enter, they sealed the hole. To fully examine the breach, the corporation called in outside teams of forensic specialists and collaborated extensively with law enforcement. Through its direct contact with impacted customers, providing them with comprehensive information about what happened and free assistance in monitoring and safeguarding against identity theft, Capital One demonstrated how seriously it regarded the breach. Capital One was seriously harmed by the hack. The most significant loss was the sharp decline in client trust, which is crucial for a bank. However, in addition to a barrage of litigation, Capital One also saw a drop in its market value. Recently, Capital One resolved one of them. The business was hit with a $80 million fine by the US Office of the Comptroller of the Currency. The regulator criticized the company's inadequate risk assessment and non-implementation of fundamental cybersecurity measures.

Lessons Learned

The Capital One data leak was a priceless teaching moment for the business as well as the larger financial industry. Capital One pledged after the event to thoroughly assess and enhance its cyber protection capabilities. The most significant improvement to its cloud infrastructure security was made, with strong access control serving as the main driver of this improvement. In addition, they started routinely scanning for weaknesses, doing away with the need to wait for the enemy to reveal gaps and switching to a more secure approach. Capital One provided even more evidence supporting cybersecurity's human component. Hills claim that the bank carried out a massive training campaign, providing employees with numerous options to enroll in courses that covered best practices for preserving cloud security as well as how to identify and fix vulnerabilities.

CONCLUSION

This week's massive data breach at Capital One is being reported similarly to several of the worst breaches of the previous ten years: one offender was apprehended who allegedly broke security and then triumphantly claimed responsibility for the fallout. After the Target and Home Depot hacks in 2013 and 2014[7], everything exactly turned out as planned. The

[7] Kuipers 2022. Data breaches and effective crisis communication: A comparative analysis of corporate reputational crises. https://link.springer.com/article/10.1057/s4 1299-021-00121-9

criminal hackers in those cases approached the compromised companies and sought money in exchange due to the public awareness of their stolen personal information. I believe that the suspect we had apprehended today was only the start of the story, much like all those earlier breaches.

SOLUTIONS AND PRACTICES

E-commerce businesses confront a variety of cybersecurity dangers that call for comprehensive and specialized security solutions due to the quickly evolving digital ecosystem. Data breaches involving customers and business disruptions will result from inadequate procedural, technological, and regulatory solutions. To put it another way, this study provides useful information and a checklist of must-do tasks for managing cybersecurity roles in e-commerce.

Robust Encryption Technologies

When it comes to transmitting or storing data, encryption is one of the most important defenses. An updated encryption system called Transport Layer Security should be implemented in order to manage and safeguard data as it passes through e-commerce. Encryption plays a crucial role in ensuring the safety of data storage and handling. Strong encryption standards prevent unauthorized individuals from intercepting or stealing data. Including all transactional data, such as payment card and personal information, and user data. Employing more robust encryption, such as the Advanced Encryption Standard (AES) with a 256-bit key, can greatly safeguard the data that is saved.

Regular Security Audits and Vulnerability Assessments

Reducing vulnerabilities requires securing the infrastructure of the e-commerce platform. Frequent vulnerability assessments and security audits are required to identify potential weak points and address them. From a robust online application to the fundamental network and outside services, the entire platform should be inspected. To identify weaknesses that might be exploited in an attack, anyone can utilize automated technologies in addition to skilled human testing. Plans must be made to eliminate hazards as soon as they are identified, and action must be taken as soon as feasible.

Multi-factor Authentication and Secure Payment Gateways

When account access is enabled using Multi-Factor Authentication (MFA), the security of that access is enhanced significantly. It becomes extremely unlikely that credentials would be compromised and allow unwanted access. PCI DSS (Payment Card Industry Data Security Standard) compliant secure payment gateways are preferred by e-commerce sites. Payment transactions will always be performed safely and encrypted thanks to PCI DSS-compliant payment gateways, lowering the possibility of payment fraud.

Employee Training and Awareness Programs

Human error is one of cybersecurity's largest weaknesses[8]. Training and awareness initiatives for staff members are the best ways to lower this likelihood. It is imperative that they possess the ability to perceive and comprehend possible hazards, like social engineering and phishing schemes. They can learn how to report and spot questionable activity through simulated exercises.

Collaboration with Cybersecurity Firms

Working with specialized small cybersecurity enterprises equips e-commerce platforms with a wealth of information and best practices. Together with ongoing support, quick oversight of the latest hazards and quick problem-solving skills are provided for whatever issues are now facing. In addition, alerts regarding potential dangers can be shared with professional industry associations or other e-commerce sites, fostering cooperation in the fight against harm.

Adherence to Industry Standards and Regulations

It is a legal need as well as a fundamental cyber skill to adhere to industry rules and laws. Industry standards that provide a framework for managing security risk in information include ISO/IEC 27001. Customers' trust and the regulation itself are dependent on compliance with regulatory requirements such as the General Data Protection Regulation (GDPR) of the European Union, which imposes specific legal accountability on businesses for what they do with their data.

[8] Dash 2022. An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.

CONCLUSION

The risks to cybersecurity that e-commerce faces are unabated. Online retailers nowadays have an extensive and ever-expanding list of tasks to complete, ranging from phishing attempts and data breaches to payment fraud and dumpster diving. There is no safe e-commerce company. When multiplied, they not only destroy the privacy of personally identifiable information but also completely destroy the confidence and trust that have grown up in digital commerce. E-commerce companies must develop a thorough, preventive strategy for cyber security that includes multi-factor authentication, frequent security audits, secure payment processing, and strong encryption in order to protect themselves. I.e. Educating employees on the value of being watchful is one initiative that businesses should take on. If every employee can take a few simple steps to ensure their online safety and contribute to preventing sensitive company data from being stolen by cybercriminals, then the business is doing something right. Examining how AI affects the kinds of threats that are posed and how they respond as AI technologies advance and become more adaptable would be a worthwhile area of future research to observe how cyber threats vary over time. Because there are so many Bitcoins hacked examples, blockchain technology may also play a significant part in the future of cyber threats. Some broad strategies to lessen cyber threats in the future might involve training older generations as well, as they tend to be less tech-savvy and are sometimes more susceptible to falling for phishing schemes or scams. The illicit or unlawful use of a computer, smartphone, or other electronic device for online purposes is known as cybercrime. Present methods must alter since cyber security will ultimately determine the future of e-commerce.