



RISK MANAGEMENT IN E-COMMERCE

Author 1: Ms. M.Sabina Yasmin,

Assistant Professors, Department of Hospital Administration, Shrimati Indira Gandhi College, Trichy-2

Author 2: Ms. K.Gayathri,

Assistant Professors, Department of Hospital Administration, Shrimati Indira Gandhi College, Trichy-2

ABSTRACT

E-commerce encompasses the buying, selling, and exchange of goods, services, and information across computer networks and the internet. Because information systems, computers, and electronic networks are critical assets, they are frequently targeted by cybercriminals. E-commerce risk management safeguards digital growth by establishing security objectives, evaluating vulnerabilities and threats, and implementing effective countermeasures. This paper presents the theoretical foundations of e-commerce risk management and analyzes a case study on Vietnam Airlines using the DREAD risk assessment model. Finally, actionable insights and recommendations are provided for contemporary enterprises aiming to enhance their e-commerce risk management practices.

Keywords: Commerce, risk management, Safeguards, Assessment, Evaluation, Improvement.

INTRODUCTION

Today's consumers and businesses have a lot of opportunities thanks to e-commerce. As a result, an increasing number of Vietnamese companies are utilizing e-commerce, creating information systems, creating websites to sell products, and offering online services. But the e-commerce growth has also given cybercriminals more room to grow. Even though e-commerce has been developing in Vietnam for more than ten years, many businesses lack experience in managing e-commerce risk. The paper analyzes how Vietnam Airlines (VNA) addressed e-commerce risk in practice after analyzing the 2016 incident and presenting some ideas of e-commerce risk management. E-commerce is trade based information. If the transmitted information does not fulfil the requirements for availability, integrity, disclosure..., the parties may suffer losses. Therefore e-commerce risk is the type of information risk related to the information and e-commerce systems are harmed and

unsafe. This relatively new term was developed as a result of an increasing awareness that the information security issue is the cause of a many of e-commerce risks that are relevant to IT. The cause is that these systems are compromised, attacked by the exploit of system vulnerabilities. There are many sources of e-commerce risk, such as computer crime, spyware, malware, adware, spyware, computer worms and computer viruses. The origin of e-commerce risk is the threat or dangerous sources, the opposing forces that can affect e-commerce transactions. The essence of e-commerce risk is the potential loss from the threat or an attack of exploiting a vulnerability. Risks are generated as a result of one or more security attacks exploiting vulnerabilities to compromise information or e-commerce system targets. As such, there may be one or several threats, but if there is no hole or no flaw, there is no information risk existence. Similarly, e-commerce systems are experiencing vulnerabilities, but if there are no exploits that exploit vulnerabilities or vulnerabilities have been patched, then there may be no risk. Briefly, risk is the intersection of e-commerce assets, threats or attacks, and vulnerabilities. In many cases, threats and attacks and vulnerabilities are often closed or tied to each other. Therefore, detecting or discovering the type of vulnerability can also help to anticipate the type and severity of threat or type of attack. Whenever, the detection of vulnerability is always a top priority in managing information risk or e-commerce risk.

Risk Management is an approach that helps in managing and make best use of the available resources. A computer code project may be laid low with an out sized sort of risk so as to be ready to consistently establish the necessary risks which could have an effect on a computer code project. It is necessary to reason risks into completely different categories. The project manager will then examine the risks from every category square measure relevant to the project.

PRINCIPLES OF RISK MANAGEMENT

There are 5 principles of Risk Management.

Global Perspective:

Larger system definitions, design and implementation is considered. The opportunity and the impact that the risk is going to have is looked. View software risks in the context of a system and the business problem planned to solve.

Forward Looking View:

Looking at the possible uncertainties that might dragged. Possible solutions of the risks that might occur in the future are considered. Think about the risk which may occur in the future and create future plans for managing the future events.

✚ Open Communication:

This enables the free flow of the communication between the end users and the development team so that they can clarify the risks. Encourage all the stakeholders and users for suggesting risks at any time.

✚ Integrated Management:

Risk management is made an integral part of the project management during this phase. A consideration of risk should be integrated into the software process.

✚ Continuous Process:

Risks are tracked continuously throughout the risk management paradigm during this phase. Modify the identified risk than the more information is known and add new risks as better insight is achieved.

RISK MANAGEMENT PARADIGM



➤ Identify

Risks are identified before major problem is created. If the risks are identified before they create a major problem then there might not be more difficulty in controlling the risks.

➤ Analyze

Deep analysis of nature, behavior and type of risk and collect information about it. It is required for the purpose of the determination of the knowledge about the risk.

➤ **Plan**

Convert the plan into actions and implementation. This phase includes the actions and implementation of the planning that was done before. After the risk detection plans are made and executed.

➤ **Track**

Necessary actions are monitored. Necessary action means the required work for the removal and minimization of the risk detected.

➤ **Control**

Correct the deviation and make necessary changes. Put the right thing in the right place and the required field will be changed according to the changes required.

➤ **Communicate**

Discussion about the current risks and the future risks and their management. Make a productive discussion between the developer and tester on the risks found in the software.

Risk management is the identification, assessment, and prioritization of risks. It followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Risk management's objective is to assure uncertainty does not deflect the endeavor from the business goals. In E-Commerce, risk management is the process of setting goals and targets for protection, analyzing threats or security attacks and exploiting vulnerabilities, assessing and ranking risk levels, and selecting countermeasures in E-Commerce enterprises or any e-commerce project.

LIST OF RISK MANAGEMENT AREAS FOR E-COMMERCE SETUP

- Asset risk relating to returns
- Asset liquidity risks
- Inadequate pricing
- Regulatory risks
- Reputation risks
- Operational risks
- Strategic risks

E-commerce risk management is crucial to any company dealing with clients or employees online - whether through a website, or even email. Proactive risk mitigation for e-commerce in both planning and development can greatly minimize costs when compared to addressing a problem after it has already taken place. Risk assessment means listing all of the risks you may face, assigning varying degrees of importance to them. The first element of the risk management process is identifying risks.

THE FIVE-STEP PROCESS FOR RISK MANAGEMENT

The following risk management steps can help your organization enhance your process of risk mitigation:

1. Identification of risks

This step involves listing out any events that would harm your business. Because it is impossible to think of all risks, you expect this step to take a couple of days or weeks. This procedure promotes cross-functional learning and collaboration. Thus, involve other departments to identify risks to have an all-encompassing risk management plan.

2. Risk analysis

This step entails choosing the area of focus. Therefore, your team will analyze the likelihood and consequences of each risk throughout this step. Accurate risk analysis depends on several factors, including time wasted, the magnitude of the effects, and the possibility of revenue loss for the business. By carefully examining each risk, you can identify problems that frequently arise throughout a project and improve the risk management procedure moving forward.

3. Risk prioritization

At this stage, you will develop and roll out plans to reduce the impact of each risk. But first, categorize each risk by considering its likelihood of occurring and any potential impact on business operations. The purpose is to assist you in finding practical solutions for each threat.

4. Establish a way to monitor risk

The risk monitoring element of the process entails tracking the status of risks, evaluating the efficacy of mitigation methods put in place, and engaging with relevant parties. It is essential to maintain clear communication with your team and stakeholders when it comes to regular supervision of possible risks.

5. Report the risk

Reporting risks helps you examine and evaluate your risk management plan and keeps them involved in risk mitigation. Companies must continuously monitor and report risk outcomes to manage them or seize unforeseen opportunities as they present themselves.

Although risks are an unavoidable part of running your business, having a risk management plan is the best way to deal with unexpected events. It helps businesses to shape their future growth while limiting risk.

RISK ASSOCIATED WITH E-BUSINESS

These risks include the unlawful sharing of data, fraud, malware, and other security breaches, not to mention vulnerabilities related to working with third-party platforms, data privacy laws, online security regulations, and customer service issues.

1. Cyber security & Data Theft

Digital platforms are prime targets for malicious actors seeking sensitive business and customer information.

- **Data Breaches & Theft:** Unauthorized access to customer credentials, personal data, or proprietary trade secrets.
- **Malware & Cyber attacks:** Ransom ware, firewall breaches, or compromised servers that corrupt data or halt business operations.

2. Payment & Transaction Risks

Online financial exchanges bring financial vulnerabilities that can lead directly to revenue loss.

- **Online Fraud & Phishing Pages:** Fake portals or deceptive pages designed to steal customer payment details.
- **Payment Failures:** Unreliable payment gateways causing declined valid orders or broken transaction chains.
- **Fraudulent Charges & Charge backs:** Unauthorized transactions resulting in financial penalties and dispute resolution costs.

3. Operational & System Downtime

E-business models depend on continuous uptime and system reliability.

- **Server Outages & System Failures:** Crashes or technical failures that make websites and portals inaccessible.
- **Loss of Service:** Temporary or prolonged disruption preventing customers from placing orders or completing transactions.

4. Legal & Compliance Risks

Operating digitally across jurisdictions requires adherence to evolving privacy laws and intellectual property standards.

- **Regulatory Violations & Fines:** Non-compliance with privacy standards (e.g., GDPR violations) leading to severe legal penalties.
- **Contract & Intellectual Property Breaches:** Trademark infringement, unauthorized content use, or breached vendor agreements.

5. Supply Chain & Logistics Disruption

An e-commerce front-end is only as effective as its physical fulfillment backend.

- **Shipping & Stock Disruptions:** Delayed shipments, warehouse backlogs, or stockouts that halt order fulfillment.
- **Broken Logistics Chains:** Third-party carrier failures affecting delivery schedules and customer satisfaction.

6. Reputation & Customer Trust

Damage to brand perception can have long-term impacts on customer retention and sales growth.

- **Consumer Backlash:** Public backlash triggered by data breaches, poor customer service, or unfulfilled orders.
- **Loss of Brand Loyalty:** Negative online reviews and poor trust scores impacting customer acquisition and repeat business.

PROCESS OF RISK MANAGEMENT

1. Establishing Risk Management Objectives

The first step in e-commerce risk management is to define the organization's risk management objectives and identify the assets that require protection. This process involves determining information security requirements and establishing priorities for managing potential risks. Although e-commerce risk management aims to ensure overall information security, organizations may prioritize specific objectives based on their operational needs. For

instance, protecting customers' personal and financial information may take precedence over maintaining uninterrupted system availability in certain situations.

2. Identifying Threats and Analyzing Vulnerabilities

The second step involves identifying potential threats and examining vulnerabilities in e-commerce systems. A vulnerability refers to a weakness in the design, implementation, operation, or management of a system that attackers could exploit to compromise security. The purpose of this analysis is to identify security weaknesses, understand how they might be exploited, and evaluate the likelihood of successful attacks. It also considers the potential sources of threats, the methods used by attackers, the possible consequences of security incidents, and the individuals or organizations that may be affected.

3. Assessing and Prioritizing Risk Levels

The third step is to assess and rank risks according to their severity and potential impact on the organization. Risk assessment can be challenging because threats, vulnerabilities, organizational objectives, and attack sources vary considerably. While some potential losses can be measured financially, others can only be estimated due to limited information or the absence of reliable numerical data. Consequently, risk assessment may involve a degree of subjectivity. Nevertheless, organizations must evaluate each identified risk and prioritize it according to its likelihood of occurrence, potential consequences, and overall impact on business operations and information security.

4. Selecting and Implementing Countermeasures

The final step is to select and implement appropriate countermeasures to manage identified risks. These measures may include security technologies, policies, procedures, and technical controls designed to detect vulnerabilities, prevent attacks, and reduce potential damage. Examples include firewalls, encryption, access controls, security updates, data backups, and incident response procedures. Organizations may also adopt recovery and restoration measures to minimize losses and resume normal operations following a security incident. The effective implementation of these countermeasures helps strengthen information security, protect customer data, and ensure the continuity of e-commerce activities.

FOUR COMMON STRATEGIES OF RISK MANAGEMENT

i) Risk Transfer

Risk transfer involves shifting some or all of the financial burden associated with a potential risk to another party. This strategy helps an organization reduce its direct responsibility for losses or damages. Examples include purchasing insurance, outsourcing certain activities, and transferring specific risks through contractual agreements.

ii) Risk Acceptance

Risk acceptance is a strategy in which an organization acknowledges a potential risk and decides to tolerate its possible consequences. This approach is generally adopted when the cost of preventing or reducing the risk is greater than the anticipated loss. However, organizations should monitor accepted risks and ensure they can manage any resulting consequences.

iii) Risk Reduction

Risk reduction involves implementing suitable measures to decrease the likelihood of a risk occurring or minimize its potential impact. Organizations may use security controls, regular maintenance, employee training, and data backup systems to reduce risks. For example, maintaining regular backups helps an e-commerce business recover important information if a hard drive fails.

iv) Risk Avoidance

Risk avoidance refers to eliminating a particular risk by discontinuing the activity that creates it or choosing a safer alternative. This strategy aims to prevent exposure to specific threats. For example, an e-commerce company may stop collecting unnecessary sensitive customer information to reduce the risk of data breaches. Although risk avoidance can be effective, it may involve additional costs or the loss of certain business opportunities.

RISK ASSESSMENT IN ECOMMERCE

The definition of a risk assessment is a systematic process of identifying hazards and evaluating any associated risks within a workplace, then implementing reasonable control measures to remove or reduce them. Risks range from hacker attacks, data breaches, website downtime, and price competition to compliance violations. To secure your online business's future, you must have a solid plan for evaluating and managing these challenges.

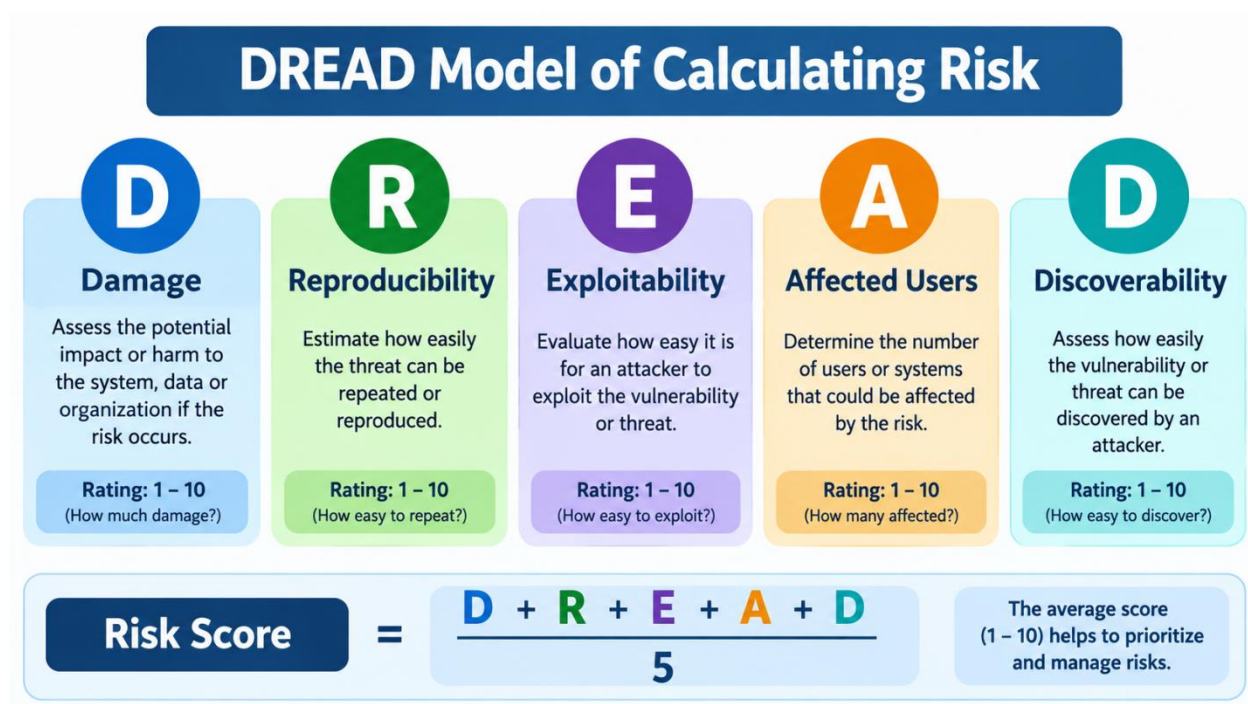
- Identify hazards.
- Assess the risks.
- Control the risks.
- Record your findings.
- Review the controls.

KEY E-COMMERCE BUSINESS RISKS

- Security issues.
- Refunds and client disputes.
- Intellectual property violation.
- Low SEO ranking.
- DDOS attacks.
- Stolen credit card information.
- Poor customer service.
- Inadequate authentication methods
- Currency exchange risks
- Customer expectations

RISK ASSESSMENT MODEL

Risk models provide the general form of the dependence of risk on dose and risk-modifying factors. Specific risk estimates are obtained by fitting the models (estimating unknown parameters) to data. The role of data in the process of risk estimation cannot be overemphasized.



DREAD is a framework that can be used to evaluate and triage various threats by rating them on an ordinal scale. The framework is broken into five main categories: Damage, Reproducibility, Exploitability, Affected Users, and Discoverability.

RECOMMENDATIONS

Information security standards and frameworks, such as COBIT 5, the ISO/IEC 27000 series, and the NIST Cyber security Framework (CSF), share common principles for protecting clients and online businesses. These frameworks help organizations identify, assess, and manage risks associated with digital information, information security, and IT systems. Implementing effective IT governance and management practices recommended by these frameworks is essential for minimizing e-commerce risks, safeguarding sensitive data, and protecting users' privacy rights.

CONCLUSION

In conclusion, various frameworks and standards have been developed to identify, assess, and manage risks in e-commerce and traditional business environments. These frameworks help protect sensitive information, ensure data security, and safeguard the intellectual property of sellers. Implementing appropriate policies and procedures enables organizations to prevent potential threats and manage risks effectively. This study applied the DREAD model to analyze VNA-related incidents and provided empirical insights into risk management in e-commerce. Other Vietnamese e-commerce businesses can learn from VNA's experience by understanding and implementing effective information risk management practices. Furthermore, organizations should adopt proactive security measures to identify vulnerabilities, prevent cyber attacks, and minimize potential damage to their operations and information systems.

REFERENCES

1. Alessandro Deidda (2009), A New Standard for Security Risk Management, ISO/IEC 27005:2008, Symantec
2. Anni Piiparinen (2016), China's Secret Weapon in the South China Sea: Cyber Attacks, <http://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/>
3. Gary Stoneburner, Alice Goguen, and Alexis Feringa (2002), Risk Management Guide for Information Technology Systems, NIST, Special Publication 800-30
4. Hengzhe Li (2011), Threat Modeling, Microsoft Security Development Lifecycle (SDL)
5. Hubbard, Douglas (2009). The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons. p. 46

6. ISO / IEC 27000: 2009, Information security management systems — Overview and vocabulary, <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-1:v1:en>
7. ITU (2015), Global Cybersecurity Index & Cyberwellness Profiles
8. Martin Petty (2016), Hackers hit Vietnam airports with South China Sea messages, <https://www.reuters.com/article/us-vietnam-hacking-idUSKCN1091YL>
9. Pooja Kungwani (2014), Risk Management- An Analytical Study, Journal of Business and Management (IOSR-JBM) e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 16, Issue 3. Ver. III (Feb. 2014), PP 83-89
10. Vietnam national assembly, Information Security Act 2015
11. William Stallings (2014), Cryptography and Network Security: Principles and Practice, Sixth Edition, Pearson
12. Wu Yanyan (2014), Research on e-commerce Security based on Risk Management Perspective, International Journal of Security and Its Applications Vol.8, No.3 (2014), pp. 153-162.