Risk Analysis of PT XYZ E-Ticketing Information with Octave Method

Ade Kartika Dewi[1], Emil R.Kaburuan*[2], Gresshinta[3], Hendrico Andre[4], Tuga Mauritsus[5]

Information Systems Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia 11480

[1]ade.dewi001@binus.ac.id, [2]emil.kaburuan@binus.edu, [3]gresshinta@binus.ac.id, [4]hendrico.andre001@binus.ac.id, [5]tmauritsus@binus.edu

Abstract

Abstract— The high demand of the community for Online Travel Agencies (OTA) services, PT XYZ as an airline and engaged in the sale of airplane tickets has developed a flight ticket sales program that has only been accessible via Desktop (DOS-based) into a WEB-based ticket sales program. By using Web Based Ticketing, the company can spread its wings by inviting agent agents in Indonesia to sell plane / hotel tickets with the Web that has been provided by the company. Ticket sales agent partners throughout Indonesia can use the PT XYZ Ticket Web portal to process flight and hotel ticket reservations. This web based IS / IT application aims to improve customer service, accuracy, speed that is in line with the company's Vision and Mission. But this must be accompanied by efforts to protect these IS / IT Assets from Risks.

One of the risks that may arise in the future is the risk of corporate information security, where information becomes an important matter and is protected from unauthorized outsiders who may be misused for certain interests and damage the information. Information is an important asset of the company which must be protected and secured.

Keywords*— information technology, assets, risk*

1. Introduction

In the era of digitizing the need for the internet to support business has become a major part of the company. A survey conducted by the Association of Internet Service Providers in 2017 showed the results that there was an increase in internet users as much as 3 times compared to 8 years ago with details of the results of the 2017 survey that the number of internet users reached 54.68% of the total population of Indonesia around 262 million people. With the development of the internet, many businesses encourage travel agents. Utilization of the internet allows the development of Online Travel Agencies (OTA) businesses. DailySocial.id conducted a survey to measure the consumption patterns of Indonesian people towards OTA consumption in 2018 with the number of respondents in 2013 and obtained the following results:

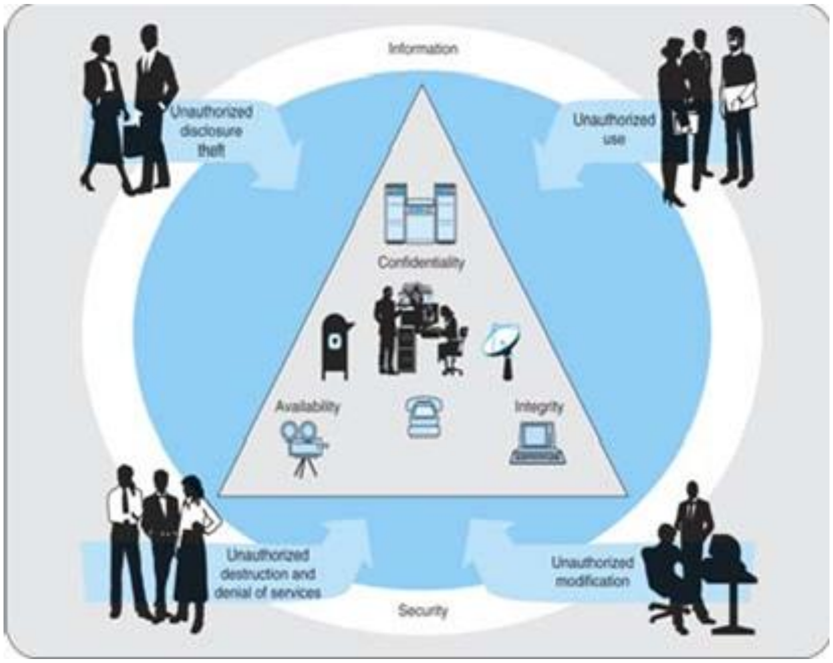
- 71.44% of respondents have used OTA services for hotel / flight ticket reservations
- 50% -70% of respondents use Traveloka / Tiket.com for flight / hotel ticket reservations.

From the high needs of the community for OTA services, PT XYZ as an airline and also engaged in flight ticket sales developed a flight ticket sales program where the old system could only be accessed via Desktop (DOS-based) into a WEB-based ticket sales program. By using Web Based Ticketing, the company can spread its wings by inviting agent agents in Indonesia to sell plane / hotel tickets with the Web that has been provided by the company. Ticket sales agent partners throughout Indonesia can use the PT XYZ Ticket Web portal to process flight and hotel ticket reservations.

Information assets (hardware, software, systems, information and people) are important assets for an organization that need to be protected from security risks from outside parties and within the organization. Information security cannot only be relied on information security tools or technology, but it needs an understanding from the organization about what must be protected and determine precisely the solution that can handle the problem of information security needs). For that we need a systematic and comprehensive management of information security. The aspects of information security needs must contain 3 important elements, namely:

1. Confidentiality: aspects that guarantee the confidentiality of data or information, ensure that information can only be accessed by authorized people and ensure the confidentiality of data sent, received and stored.
2. Integrity: aspects that guarantee that the data does not change without the permission of the authorities (authorized), must be maintained the accuracy and integrity of information
3. Availability: aspects that guarantee that data will be available when needed, ensuring that authorized users can use the information and related tools when needed.

Three aspects of security are vulnerable to threats of attacks that threaten the existence of both attacks on information sources both physically and through network access. To overcome security risks, it requires the ability to manage / manage information security risks. Therefore, a management science approach is needed.


Information
Unauthorized disclosure theft
Unauthorized use
Confidentiality
Availability
Integrity
Unauthorized destruction and denial of services
Unauthorized modification
Security

2. Literature Review

2.1. Information Technology

Understanding information technology in general is a study of design, implementation, development, support or management of computer-based information systems, especially in the application of hardware (hardware) and software (computer software). Simply put, the understanding of information technology is the facilities consisting of hardware and software in supporting and improving the quality of information for every level of society quickly and quality. Meanwhile, according to Wikipedia, the understanding of Information technology (IT) is a general term of technology to assist humans in making, changing, storing, communicating, and disseminating information. The purpose of information technology is to solve a problem, open creativity, increase effectiveness and efficiency in human activities.

2.2. Information System

Information system, an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products. Business firms and other organizations rely on information systems to carry out and manage their operations, interact with their customers and suppliers, and compete in the marketplace. Information systems are used to run interorganizational supply chains and electronic markets. For instance, corporations use information systems to process financial accounts, to manage their human resources, and to reach their potential customers with online promotions. Many major companies are built entirely around information systems.

Figure 1. Three Elements of Information Security Aspects

2.3. Information Systems Security Management Framework (ISMPF)

The ISMF provides a framework for an assured information security environment, utilizing risk management and other processes and principles

The objectives of the ISMF are to: support the attainment and realization of three information security objectives across Government: Confidentiality (including information the Government keeps about members of the public), Integrity and Availability of information and Availability of information

The evaluation of activities considers what happens during the evaluation, when an organization evaluates information security risks, then to carry out activities:

1. **Identification**
   Identify information security risks (record risk profile and organizational information)
2. **Analysis**
   Analyze risks to evaluate risks and determine priorities.
3. **Mitigation Plan**
   Plan ways toimplement a risk protection and mitigation strategy from a detailed development plan by evaluating the action plan. This activity can include a detailed cost-benefit analysis between strategy and action.
4. **Implementation**
   Implement the selected action plan in detail
5. **Monitor**
   Monitoring progress and effectiveness, this activity includes monitoring risk for each change

6. **Control**
   Control the implementation in accordance with corrective actions, by analyzing data, making decisions and executing the results of decisions made.

This cycle is carried out on an ongoing basis related to the increase and increase of risks that always appear to threaten information security. General Accounting Office (GAO) makes guidelines in managing risk as shown below [6] :

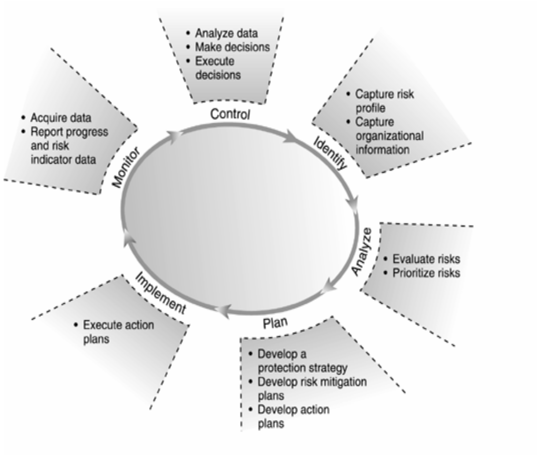


Figure 2. Framewoek Cycles based on GAO, 98

2.4. OCTAVE methodologies

OCTAVE methodologies were merely created to tackle the information security challenges faced by the U.S. Department of Defense (DoD), but as it has shown its effectiveness, now this methodology is open for public. The main aim of OCTAVE is to help organizations ensure that their goals and objectives are connected with their information security activities.

To manage information security risk is to recognize whether the risk of the organization implementing it. After the risks are identified, the organization can make a plan for mitigating and reducing / mitigating risks to each known risk. The OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation) method developed by the Software Engineering Institute, Carnegie Mellon University, 1999 allows organizations to do the above.

OCTAVE is an approach to evaluating information security risk that is comprehensive, systematic, directed, and carried out on its own[4]. The approach is arranged in a set of criteria that defines the essential elements of information security risk evaluation. OCTAVE criteria require evaluation which must be carried out by an interdisciplinary team consisting of information technology personnel and business organizations. Team members work together to make decisions based on risks to the organization's critical information assets. Finally, the OCTAVE criteria require cataloging information to measure organizational practice, analyze threats, and develop protection strategies and this catalog becomes a source of knowledge databases. This catalog includes:

1. catalog of practices – a collection of information security strategies and practices
2. generic threat profile – a collection of common threat sources
3. catalog of vulnerabilities – a collection of weaknesses based on platform and application

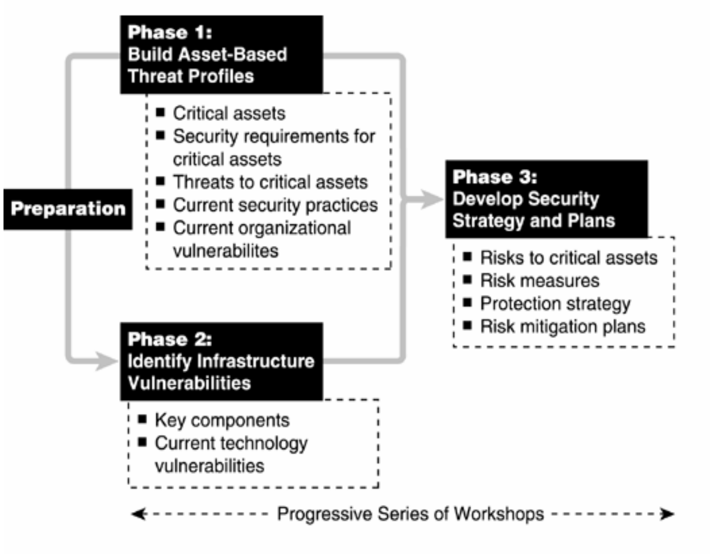

Phase 1:
Build Asset-Based
Threat Profiles
■ Critical assets
■ Security requirements for critical assets
■ Threats to critical assets
■ Current security practices
■ Current organizational vulnerabilites
Preparation
Phase 3:
Develop Security
Strategy and Plans
■ Risks to critical assets
■ Risk measures
■ Protection strategy
■ Risk mitigation plans
Phase 2:
Identify Infrastructure
Vulnerabilities
■ Key components
■ Current technology vulnerabilities
Progressive Series of Workshops

Figure 3. OCTAVE Method

Using a three-stage approach, the OCTAVE method examines organizational and technological issues against the compilation of comprehensive problems based on an organization's information security needs [5]. OCTAVE stages are :

a. **Preparation phase**

At this phase, preparatory activities must be carried out before implementing the OCTAVE method. arrange a schedule, form an analysis team, request support and prepare logistics.

b. **Phase 1: Building a profile-based Asset threat**

The output of this stage is:

- Assets that are important to the organization
- The security needs of important assets which are inseparable from the 3 aspects of security namely confidentiality, integrity and availability.
- The current security practices of the organization or the organization's efforts to protect information assets
- Current weaknesses in organizational policies.

c. **Stage 2: Identification of Vulnerability Infrastructure**

This is an evaluation of computer network infrastructure information. Key operational components of the information technology infrastructure (servers, PCs, laptops and network devices) identified weaknesses both in terms of technology and configuration, which can lead to security access by unauthorized people becomes easy

d. Stage 3 : Developing Security Strategies and Planning.

The output of this stage is:

- Risks to important assets
- Measuring the level of risk
- Protection strategy

3. Research Methodology

IT Risk Analysis at PT XYZ is carried out by applying the OCTAVE methodology. As explained in Chapter II, the OCTAVE Method has three phases that begin with the Preparatory activities. Data collection was carried out through observation, document review and with direct interviews with the management of PT XYZ especially IT Managers. The phases in the OVTAVE method and the activities carried out from each phase are as follows:

A. Preparation

Preparations made were to arrange a schedule, form a risk analysis team consisting of Researchers, IT Managers of PT XYZ, User Online Ticketing representatives from each branch in the region. Conducting Literature Studies, conducting Protocol interviews and interviews

B. Phase 1 : Building Asset Based Profile Threats

Processing data obtained from the Preparation phase. The output of this phase is a list of PT XYZ's important assets, especially related to Web Based Online Ticketing, a list of security needs at PT XYZ (Confidentiality, Integrity and Availability), a list of threats, a list of security that has been applied and a list of weaknesses of PT Web Based Online Ticketing XYZ

C. Phase 2 : Vulnerabilities Infrastructure Identification

At this phase, identification of weaknesses in terms of PT XYZ's Web Based Online Ticketing infrastructure as IS business support for PT XYZ. The output obtained from this phase is a list of key components and vulnerabilities or weaknesses of the key components.

D. Phase 3 : Develop Security and Planning Strategies.

The activities carried out in Phase 3 are to carry out the process of identifying risks from crisis assets, actions on risk, protection and mitigation plans. The output obtained from this process is a list of risk impacts, risk protection and mitigation from PT PT XYZ.

4. Result and Discussion

4.1. Preparation

Based on the results of interviews and observations obtained the existing conditions of assets that support the business of PT XYZ. In running its business, PT XYZ uses software created by the IT team for the process of recording ticket sales and also uses payment gateway software from vendors. From each branch to access the ticket sales web application through the internet network. The web application is stored on a server which can then be accessed publicly via the internet. Following is the network architecture used by PT XYZ at each branch in Jakarta, Tangerang and Bekasi

4.2. Phase I Building Profile Based Asset Threats

PT XYZ has ticket sales agents located in Jakarta, Tangerang and Bekasi. PT XYZ's critical assets are categorized as hardware and software. For each Jakarta, Tangerang and Bekasi branch in the hardware category there are Servers, Client PCs, Firewalls, UPS, internet networks, Routers, Switches & Modems. While in the software category there are Windows Operating Systems, Payment Gateway Systems from vendors, and Antivirus.

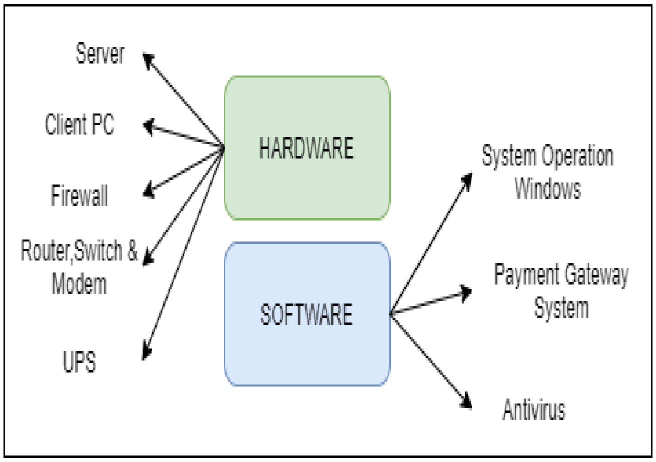


Figure 4 .Hardware and Software at PT XYZ branch

Identification of weaknesses from the organization including knowledge of IT owned by the user or the operational team (customer service ticket) is inadequate. Ticket customer service depends on the system provided to support the work.

4.3. Phase II Identification of Vulnerabilities Infrastructure

At this stage, identification is carried out at the infrastructure level of PT XYZ as part of supporting the use of assets. From the identification of infrastructure assets there are key asset components, namely Server, Router, Computer and network. After doing the next identification is to analyze the vulnerability / weaknesses of these assets into the table as follows:

Table 1.List of Asset Weaknesses

No	Keys of Assets	Weakness
1	Router	The placement of routers in each branch is in the same room where the customer arrives. Making it possible for damage by outsiders.
2	Server	The server used is combined with other applications so that if there are obstacles to other applications it will have an impact on the ticketing application.
3	Computer	Protection currently uses a Windows-based OS with antivirus support that is not routinely updated
4	Network	The network used utilizes public access that is vulnerable to attacks from outsiders.

4.4. Phase III Developing Security and Planning Strategies

After obtaining the key components and their weaknesses at this stage the risk identification process of PT XYZ's IT assets is carried out. There are four types of actions in dealing with risk, namely :

a. Take, the act of accepting the risk that exists because the risk is unavoidable such as an unavoidable natural disaster.
b. Treat, the act of taking direct steps to reduce the impact of risks
c. Terminate, action to stop the risk
d. Transfer, transfer of risk to other parties, for example, transferred to the insurance.
e.

Table 2 .List of Risks in the Hardware category

No	Risk	Cause	Action	Mitigation
1	Server Damage	Configuration error	Treat	There is a proper procedure in the configuration process
		Virus attack	Treat	The existence of antivirus on the computer server and firewall is always updated every 3 months
		Age of Hardware	Treat	Perform regular and scheduled data backups
		Natural disasters	Take	Setting up a fire extinguisher on the server Setting up a Disaster Recovery Center (DRC)
2	Computer	Virus attack	Treat	The existence of antivirus on the computer server and firewall is always updated every 3 months
		Age of Hardware	Treat	Perform regular and scheduled data backups
		Error in Operating System Installation	Treat	Conduct training on IT teams in computer installations according to company standards
		Data theft	Treat	Make credentials for each account according to their responsibilities.
3	Router	Age-related damage has taken too long	Treat	Router rejuvenation every few years
		Electric short circuit	Take	There are fire extinguishers in every room
4	UPS	Damage due to damaged / worn out battery	Treat	Check battery life periodically on the UPS
		Natural disasters such as fire	Take	There are fire extinguishers in every room
5	Network	Cable disconnected	Treat	Install cable protectors
		The cable is not installed properly	Treat	Conduct training on IT team in cable management
6	Switch	Damage to switch port	Treat	Use a switch with good electrical grounding

		Age-related damage has taken too long	Treat	Rejuvenation switches every few years

After knowing the risks and providing action on each of these risks for the hardware category just use the Treat and Take approach. Next is to identify the risks in the software categories in the following table:

Table 3 .Risk Mitigation in the Software category

No	Risiko	Penyebab	Tindakan	Mitigasi
1	Operation System failure	Hardware is not working properly like RAM and hard drive is damaged	Treat	Routine maintenance on each computer and performing scheduled backups.
		Virus attack	Treat	Make a restore point on the computer to make it easier to restore the configuration before a virus attack. Update antivirus regularly every 3 months.
		Software failure	Treat	Perform regular and scheduled data backups
2	Disruption to the payment gateway system	The software license has expired	Transfer	Make a reminder to contact the vendor before the license runs out.
3	Interference with supporting software	There is a virus attack on supporting software	Treat	Update antivirus regularly every 3 months.
		Endless software support from the developer	Treat	Looking for alternative similar software

In the software category, action is carried out using the Treat and Transfer approach. Treat measures are taken to risk operating system failure, virus attacks, software failures and endless software support from the developer. While the transfer of risk for the cause of endless software licenses from vendors.

5. Conclusion

Identifying threats and risks at PT XYZ is one of the success factors for the company in running its business. By identifying threats and risks it can minimize the worst that might happen in the future. There are 9 risks consisting of hardware and software categories with each cause that can be minimized by impacting the Treat, Take and Transfer measures. The results of risk and mitigation can be used as a reference by companies to prevent or handle the risk of assets of PT XYZ.

References

[1] M.J. Culnan, The intellectual development of management information systems, 1972±1982: a co-citation analysis, Management Science 32 (2), 1986, pp. 156±172. K. A. Endaya and M. Mohd Hanefah, “Internal Audit Effectiveness: An Approach Proposition

to Develop the Theoretical Framework," *Res. J. Finance. Account.*, vol. 4, no. 10, pp. 92–102, 2013.

[2] Office of the Chief Information Officer, "Information Security Management Framework OCIO/F4.1," no. September, pp. 1–226, 2014, [Online]. Available: http://dpc.sa.gov.au/sites/default/files/pubimages/documents/ocio/ISMF_v3.pdf.

[3] Niklas Möller, 2018, Handbook of safety principles,Hoboken, NJ : Wiley

[4] Alberts, Christopher and Dorofee, Audrey, Managing Information Security Risks: The OCTAVESM Approach, 2002.

[5] Alberts, Christopher and Dorofee, Audrey. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVESM) Criteria (CMU/SEI-01-TR-016). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. Available online: <http://www.sei.cmu.edu/publications/documents/01.reports/01tr016/01tr016abstract.html

[6] United States General Accounting Office. Executive Guide: Information Security Management (GAO/AIMD-98-68). Washington, DC: GAO, 1998