

CHAPTER 1 – INTRODUCTION

1.1. Background

As digital transformation in the media industry increases, companies are increasingly relying on information technology (IT) for the production, distribution, and storage of digital content. From content production and distribution to audience engagement, everything depends on a reliable and secure IT system (Khandelwal et al, 2020). By (Indrati, Mani and Aras, 2018) in his research entitled Challenges to Mass Media Posed by Convergence in the Indonesian Context examines the various challenges faced by Indonesian mass media in facing the era of media convergence. Through a case study on Metro TV, this study reveals how convergence requires significant changes in organizational structure, editorial work patterns, and journalist competencies. One important finding shows that the process of integrating newsrooms into one unit called the Super Desk requires adaptation that is not only technical, but also cultural in the work environment. Journalists are required to have multiskill abilities in order to produce integrated content across various platforms, such as television, online news portals, and social media. However, the implementation of convergence also faces obstacles, including internal resistance, limited training, and infrastructure that is not yet fully adequate. This study emphasizes the importance of change management strategies, increasing human resource capacity, and strengthening cross-divisional collaboration as crucial steps to effectively face the challenges of media convergence in Indonesia. However, dependence on information technology in responding to convergence challenges in media companies also increases exposure to cybersecurity risks.

Cybersecurity has become an important problem for the media industry, because valuable assets such as intellectual property, news content, and company reputation are vulnerable to cyberspace threats (Yadav and Dong, 2014). The threat of cyberspace faced by the media industry can include hacking attacks, data theft, dissemination of fake content, and information technology disorders that can hamper business operations (Zafar *et al.*, 2021). In addition, vulnerability in information technology systems, such as the weaknesses of software security used, inadequate configurations, and lack of user

safety awareness, can function as an entry point for cyber criminals (Alazab and Broadhurst, 2016).

The impact of cyber security incidents in the media industry can be very significant, ranging from financial losses and operational disorders to damage to the company's reputation (Cremer *et al.*, 2022). Therefore, a comprehensive and effective cybersecurity strategy is crucial to protecting the media industry's infrastructure from threats and vulnerabilities. According to the Global DDoS Report 2024: Distribution of Industries Attacked by DDoS Attack Groups, the importance of cybersecurity against DDoS attacks for organizations lies in their direct impact on service availability. The report indicates that the financial, e-commerce, public services, and media sectors are prime targets. Without adequate protection, organizations risk operational disruptions, financial losses, and loss of customer trust due to continued service unavailability. Therefore, companies need to implement a comprehensive cybersecurity strategy to protect their digital assets and businesses.

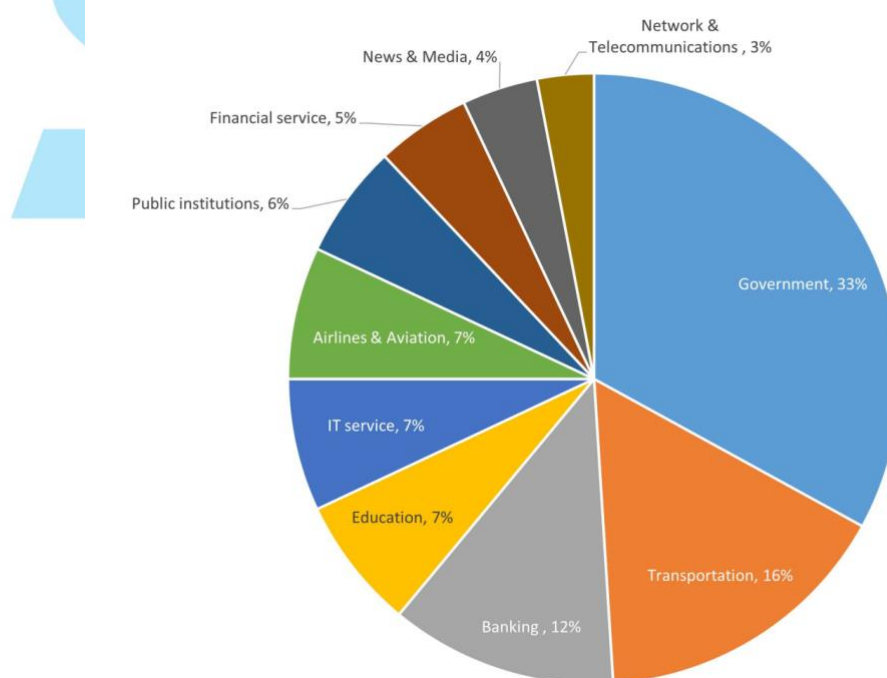


Figure 1.1. Distribution of Industries Attacked by DDoS Attack. (NSFOCUS, 2024)

In Figure 1.1. shows that many companies experience increasing cyber attacks such as DDoS attack every year, so media companies facing big challenges in protecting

systems that must remain and important information, especially those related to journalistic activities. Journalists often work with data, such as sources of information, internal documents, or ongoing investigations. If this information system service stops, the impact can be very detrimental, for the media company itself. According to research by (Gakh *et al.*, 2024), journalists are often the target of cyberspace attacks because of their role in expressing sensitive information and the system used is the target of attacks. Therefore, knowledge about the threat, risk, and mitigation models in applications used by journalists is very important to ensure the security of information integrity.

A threat model is a framework used to identify potential threats to a system or application. In the context of applications for journalists, a threat model helps identify vulnerabilities that may be exploited by irresponsible parties. For example, threats such as hacking, phishing, or malware attacks can threaten the security of journalists' data. According to (Shostack, 2014), threat modeling is an important step in developing a secure system because it allows the security team to map potential threats and design appropriate defenses.

In addition to the threat model, risk assessment is also an important component in this research. Risk assessment helps media companies measure the extent to which the identified threat can affect the company's operations and reputation. For example, if an application used by journalists is vulnerable to cyber attacks, the risk faced is not only that data cannot be sent to editors, but also financial losses and decreased public trust due to the obstruction of information to the public. According to (Stoneburner, Goguen and Feringa, 2002), risk assessment is an important process for determining the priority of mitigation and allocation of security resources. By conducting a risk assessment, companies can prioritize the most effective mitigation steps to reduce this negative impact.

The following are some types of cyber attacks on the media industry:

1. Distributed Denial-of-Service (DDoS) Attacks.

DDoS attacks can cause broadcast service disruptions by overwhelming network infrastructure, resulting in financial and reputational losses. (NSFOCUS, 2024)

2. Ransomware Attacks.

Malware that encrypts critical data and demands a ransom, disrupting broadcast operations and content distribution.(Malik *et al.*, 2023)

3. Content and Sensitive Information Leaks.

Theft or leak of proprietary content, such as scripts or pre-release videos, can be financially and reputationally damaging. (Khan, 2024)

4. Vulnerabilities in Digital Broadcast Infrastructure.

The integration of IP technology into broadcasting increases the risk of cyberattacks targeting digital infrastructure. (Malik *et al.*, 2023)

In the digital era, based on the risks above, PT. XYZ as a television media company faces major challenges in maintaining its relevance and competitiveness.. Changes in consumer behavior that are increasingly shifting to digital platforms, such as streaming and social media, have shifted traditional content consumption patterns. According to research by (Doyle, 2016), media convergence is an important solution for television companies to integrate traditional platforms with digital platforms, so that they can reach a wider audience and increase engagement. Convergence solutions not only allow television companies to provide content through various channels, but also open up new opportunities in monetization, such as data-based advertising and subscription services. Without adopting a convergent business model, television companies risk losing market share and revenue. In addition, according to research by (Jenkins, 2008), media convergence is not only about technology integration, but also about cultural and operational transformation within the company.

Previously, PT.XYZ used the File Transfer Protocol (FTP) method to send videos from field journalists to the head office. While the text is sent via email or platform chat to the editor separately. This will make it difficult for other platform editors such as newspapers or editor of the news portal website to take news resources because there is no text in the video. In addition, each editor has a different system, television editor with the ftp method, newspaper editor with their own system, editor of the news website with their own system. This requires a centralized system that can accommodate all editorial systems in one application so that applications become the manifestation of media convergence to the digital era. By applying convergence solutions, television companies can create improved content efficiency, and optimize distribution. One of them is the

implementation of the Content Management System (CMS) application, which is the software used to create, manage, modify, and publish centrally digital content. PT.XYZ, CMS plays an important role in managing various types of content, such as news articles, videos, images and interactive content into one, which is then distributed through various platforms, including websites, television, newspapers, and social media. As revealed by (Küng, 2017), a media company that successfully adopted convergence will have a competitive advantage in dealing with changing times. Therefore, the availability of a convergence application system solution is an urgent need for television companies to survive and develop in this challenging digital era.

The importance of CMS PT. XYZ as a crucial asset for television companies because it plays a central role in the process of collecting, producing, and distributing news content. However, dependence on information technology and digital systems makes CMS vulnerable to cybersecurity threats, such as ransomware attacks, data leaks, or deliberate system disruptions. These risks can not only disrupt the company's operations, but also damage the reputation and public trust which are very valuable intangible assets for television companies.

Therefore, the television company PT. XYZ depends on the Content Management System (CMS) to manage, store, and distribute journalistic content quickly and efficiently. CMS becomes an operational backbone for journalists, editors, and production teams in delivering news to the public. However, cyber threats to CMS media companies continue to increase, such as hacking news data, content manipulation, DDoS attacks, and theft of journalist identity (see appendix 13 and appendix 14). In addition, cyber attacks that cause downtime CMS can interfere with news production process, damage the company's reputation, and have an impact on finance and public trust. To overcome this threat, threat modeling and risk assessment are needed as a proactive strategy in identifying, analyzing, and mitigating risks that can affect media operational sustainability.

To analyze threats effectively, threat modeling can be used as a method for recognizing potential risk and threats in the content management system. Threat modeling is a systematic approach that aims to identify security gaps and potential attacks, evaluate

the level of risk caused, and determine priorities in the application of mitigation steps to protect infrastructure from possible attacks (EC-Council, 2024).

This research focuses on determining risk by threat modeling, risk assessment and mitigation of threats to important assets of the CMS application that aims to ensure media operational sustainability and compliance with privacy law in television companies in reducing the risks of cyber security of PT. XYZ.

1.2. Research Problem

Based on Figure 1.2, there are two major problems in the Journalist Content Management System Application (CMS), namely **Security Vulnerability Application** and **Operations Issues**. The research problem lies in overcoming an increase in the risk of cyber attacks and potential data violations in important company asset media platform such as news article, video and photo. This challenge is strengthened by the accessibility of platforms to internal journalists and the writer contributor, expanding the potential surface of the attack.

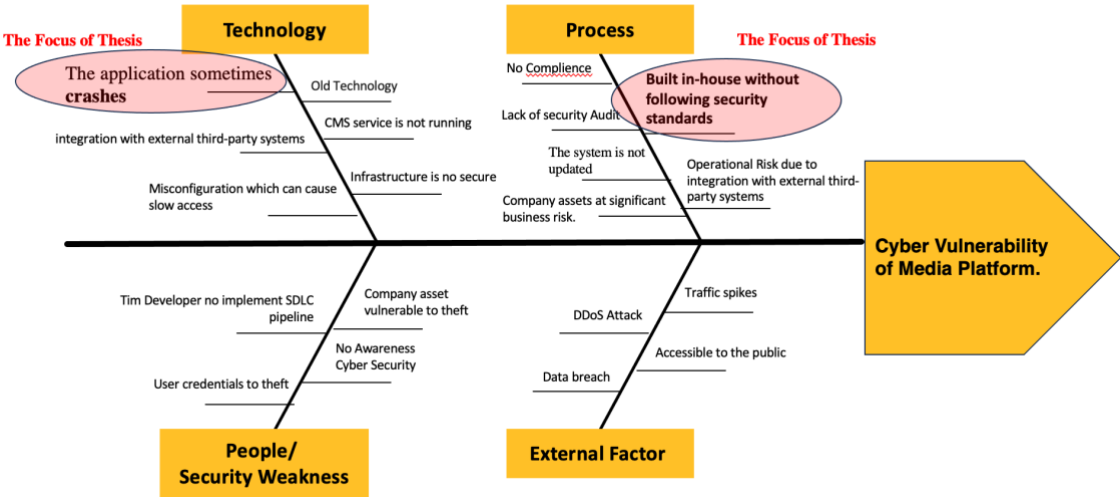


Figure 1.2. Research Fishbone Diagram.

The platform's vulnerability stems from being built in-house without following security standards, leading to fundamental weaknesses. Poor system audits and reliance on outdated technology make it prone to attacks. Integration with third-party systems adds more risks, exposing data to threats like SQL Injection, XSS, and

malicious uploads. There's also a risk of credential theft. Beyond security, operational issues like slow performance during traffic surges, misconfigurations, and CMS failures disrupt content delivery. (See appendix 17)

This research aims to identify problems by modeling threats and assessing the risk of threats to CMS applications. Then the proposed countermeasures will be described to overcome this threat and identify any gap. This is intended to ensure alignment with information security standards guidelines so that CMS service operations can continue to support the business of PT. XYZ.

1.3. Research Objective

This research aims to enhance dan resilience Media News Application PT.XYZ security posture and security compliance by developing a comprehensive risk assessment tailored for content management system.

The following research objectives are for this master thesis :

1. Develop a risk assessment threat model framework to content management system application and maintains the operational sustainability of media.
2. Conduct a detailed risk analysis to indentify threat key and vulnerability in Content Management System at PT.XYZ
3. This research will provide strategic risk mitigation and compliance recommendations with OWASP Top 10 and ISO 27001:2022 to support operational sustainability of media and UU PDP for protection of personal data.

1.4. Research Question

In accordance with the aim of this research, this is the research question :

1. How can a threat modeling risk-based approach improve the security and operational issues of the Journalist Content Management System (CMS) at PT. XYZ ?
2. What are the most critical security vulnerabilities present in the CMS as a result of threat modeling to effectively identify, assess, and prioritize these risks?

3. What specific strategies and controls can be developed from the findings of the risk assessment model to mitigate risks PT. XYZ's CMS for technical staff and management ?

1.5. Hypothesis

1. **Hypothesis 1:** Designing a structured threat modeling framework will help application developers improve CMS overall security posture.
2. **Hypothesis 2:** The CMS's critical vulnerabilities directly compromise data integrity and confidentiality, exposing PT. XYZ to reputational and regulatory risks.
3. **Hypothesis 3:** The strategies and controls developed from the Risk Assessment Model will effectively mitigate risks in PT. XYZ's CMS application. This strategy will improve the company's security and be in line with cybersecurity standards to maintain operational sustainability so that it can have an impact on the company's business.

1.6. Research Scope and Limitation

The scope of this research work is determined as follows :

1. The research examines PT.XYZ security gaps by analyzing the efficiency of existing safeguards and suitability in mitigating known security threats with proposed designing a threat modeling.
2. The scope of this research is focused on the application of risk assessment on critical company assets such as CMS applications at PT.XYZ. This application is used by journalists to process news content which will then be used on several media platforms. This research focus threat modeling on business process of CMS.
3. This research aims to proposed improved security control recommendation plan to mitigating the risks of PT XYZ applications in accordance with cybersecurity compliance and personal data protection and minimize security risk in technical and management perspective.

Limitations :

1. The research focus on the website application content management system of media platform PT XYZ.
2. This research defines threats with various threat models integrated only process bussiness of CMS and threat analysis method based on risks centered and combined with business objectives and requirement techniques for comprehensive risk analysis.
3. The proposed cybersecurity enhancement method will be evaluated in a controlled environment using security events and selected datasets from enterprise cms applications. Full scale implementation and impact of this control will be part of the future research agendas.
4. Mitigation control recommendations for the resulting risks are based only on mitigation controls in accordance with ISO 27001:2022 and OWASP Top 10 guidelines.
5. Access to sensitive data and information related to actual threat incidents within the organization may be restricted, which could hinder a thorough analysis of real-world scenarios.

A well defined scope and limitation allow research to remain focused and realistic, while opening up opportunities for further development in strengthening future cybersecurity systems.

1.7. Significance of Study

The contribution of this research is :

1. Contributing to the discovery of threats and potential risks of implementing CMS applications at PT.XYZ which can increase the effectiveness of security and privacy risk analysis.
2. Providing recommendation and control to reduce threats and risks in CMS Application to support operational sustainability of media and compilience with the privacy law in PT.XYZ.
3. Contribution to the development of integrated threat models.
4. A methodology that can be replicated and applied to other systems.
5. Contributing strengthening threat modeling practices in the devsecops pipeline.

1.8. Thesis Structure

This thesis is written following the structure start from chapter 1 and end in chapter 5

- Chapter 1 is Introduction, discussing the background, problem definition, objective, question, scope, significant of study and hypothesis which motivate and focusing this thesis area.
- Chapter 2 is Literature Review, discussing the finding during papers survey related the thesis topic and also with the hypothesis, including the idea, conceptual description and critical review of the previous work documented in the published paper of the science journal or conference .
- Chapter 3 is Research Methodology, describe the Methods and Frameworks to be used to examine the Hypothesis and answer the research questions.
- Chapter 4 is Result and Discussion, discussing the fact finding, information finding from data processing including the experiment and comparison study with the previous work. Relation of the information finding with the hypothesis also covered in this chapter.
- Chapter 5 is Conclusion and Recommendation, discussing the summary and conclusion which relates all the exploration from the beginning to the finding during experiment. And base on the conclusion, recommendation of novelty in method aspect, theoretical or future work is proposed.