

Chapter 1

INTRODUCTION

1.1 Background

In this age of rapid innovation, the digital realm is transforming at an extraordinary rate, powered by fast-paced technological developments and the deep integration of digital systems into nearly every area of human activity. As shown in Figure 1.1, by 2024, there are 5.35 billion internet users, representing 66.2% of the global population. Over the past year, internet usage has grown by 1.8%, with 97 million new users coming online for the first time in 2023.

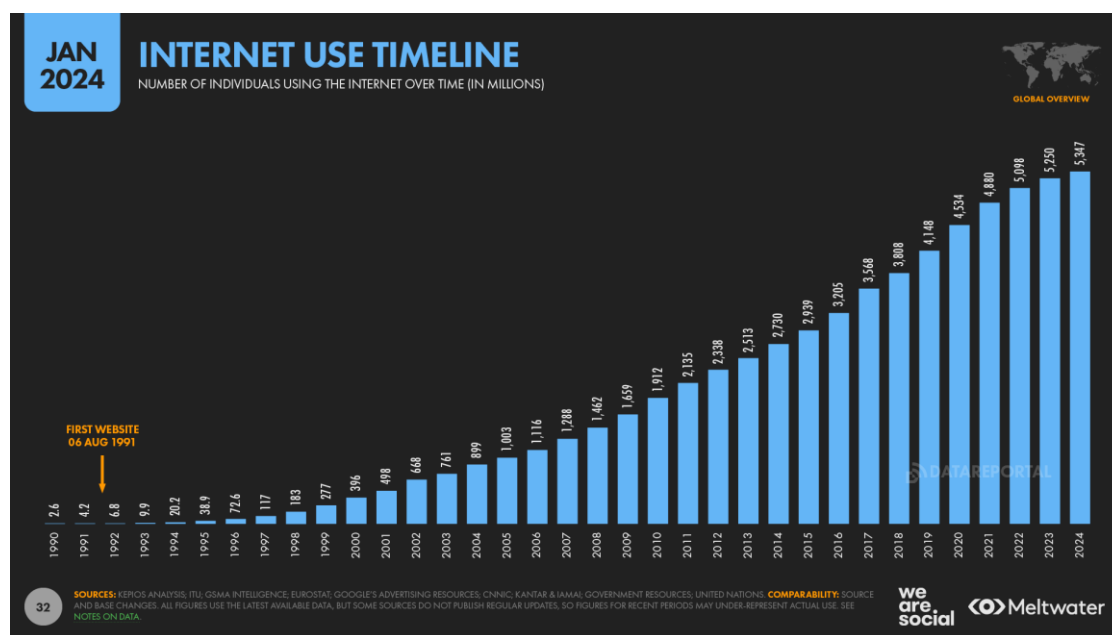


Figure 1.1: Internet Use Timeline (Kemp2024)

With the growing number of internet users, industries in every sector are increasingly dependent on technology to foster innovation, boost efficiency, and stay competitive. This requires organizations to be agile and scalable, staying up-to-date with the latest technological advancements. To effectively manage these challenges, executives must align their long-term technology adoption plans with both internal capabilities and external market conditions, ensuring the seamless integration of new technologies into their business models. (Yee et al,2024)

The widespread adoption of technology across various industries for business development has inadvertently fueled a surge in cyberattacks. On the X-Force Threat Intelligence Index 2024 (IBM X-Force 2024) observed that in 2023, there was a notable increase in cyber threats targeting identities. Historically, attackers have preferred the path of least resistance to achieve their goals. Today, the emphasis has shifted from hacking into systems to simply logging in, reflecting the relative simplicity of obtaining credentials compared to exploiting vulnerabilities or carrying out phishing attacks. This trend was supported by IBM X-Force penetration testing data for 2023, which identified identification and authentication failures as the second most common issue.

Mapping with Top OWASP web application security risk as shown on the Figure 1.2. Identification and authentication failures accounted for 21% of the most common web application security risks. Among these, the leading issues included weak password policies, such as those tied to Active Directory (19%), errors that allowed username verification (17%), and both the lack of required Server Message Block (SMB) signing and URLs containing sensitive information, each at 8%.

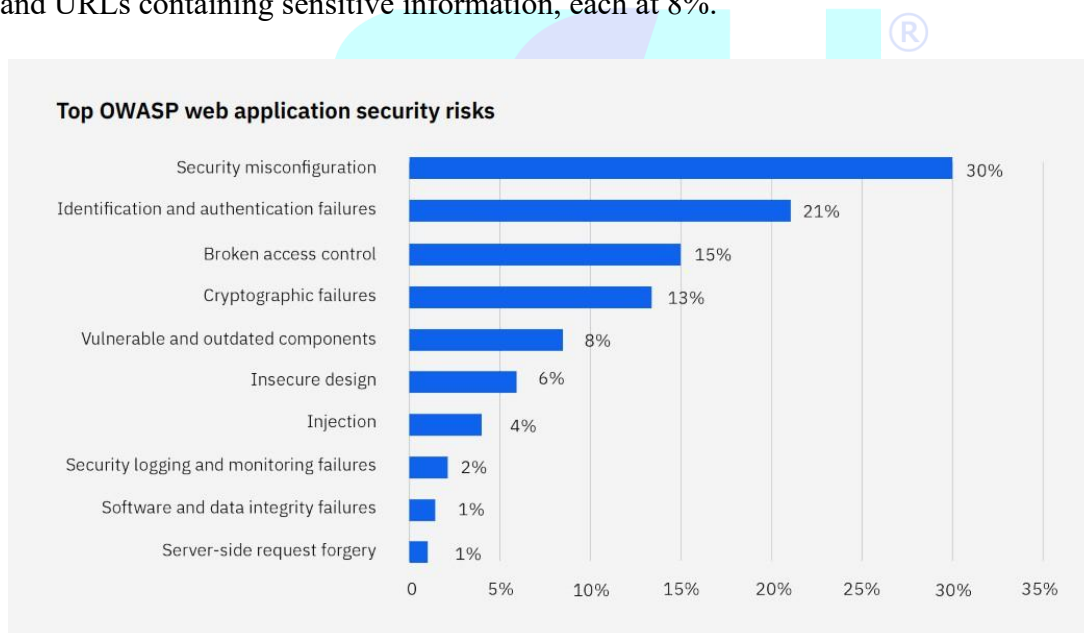


Figure 1.2: Top OWASP web application security risks based on X-Force penetration testing data. (IBM X-Force 2024)

Between 2011 and 2020, can be shown on the Figure 1.3 there has been a clear and consistent rise in data breaches, characterized by an annual increase in both the frequency of events and the amount of exposed data. This increase underscores the crucial necessity for enterprises to strengthen their defenses and aggressively protect

their assets against possible assaults.

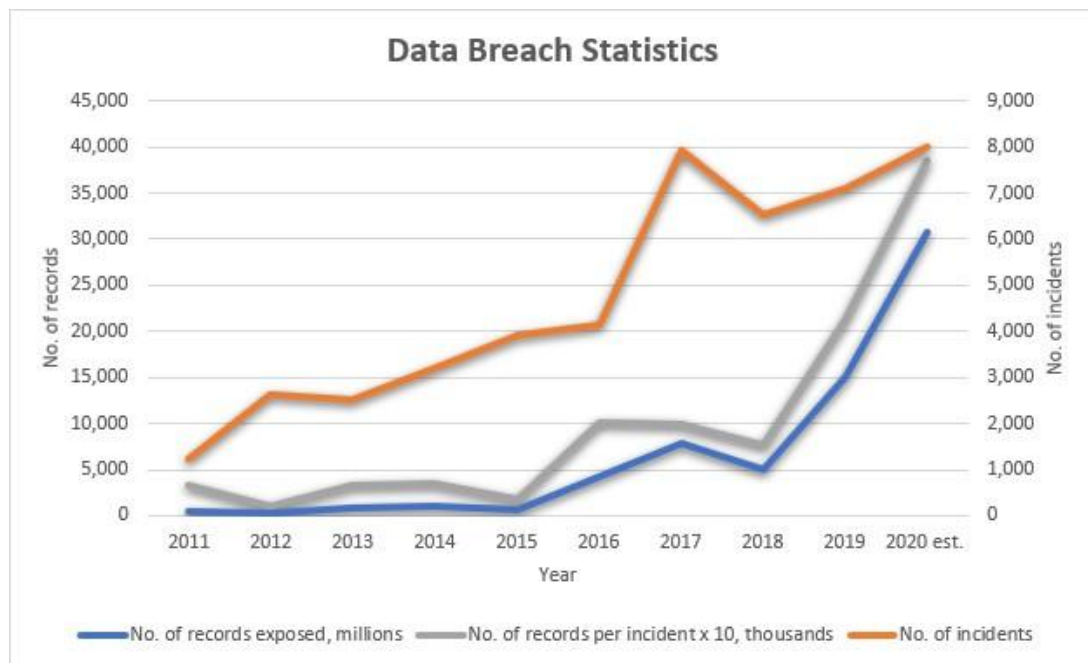


Figure 1.3: Data Breach Statistics (Perry 2019)

The 2021 Data Breach Investigations Report conducted by Verizon analyzed over 79,000 security incidents and detected 5,200 instances of data breaches. An important discovery was that stolen credentials were a critical factor in more than 60% of these attacks. Furthermore, the survey indicated that in 85% of the cases, human involvement played a role, underscoring the importance of human-related variables in security incidents. Remarkably, a mere 3% of the incidents were associated with breaches that took advantage of weaknesses in the system (Branka 2023).

In addition to heightening the sense of urgency, Indonesia government created the Law related the protection of the personal data called the Personal Data Protection Law (UU PDP) and scheduled to be implemented in October 2024. Given the forthcoming rule, enterprises must conform to the UU PDP criteria and establish strong safeguards to avert data breaches. Emphasis should be placed on protecting consumer data, particularly information that includes Personally Identifiable Information (PII). Following these guidelines is crucial for preserving the security and integrity of sensitive information.

In the era of digital transformation, PT XYZ is strategically advancing its business by transitioning to a digital-first approach. This involves developing applications

designed to enhance government digitalization efforts upon request, as well as creating apps that streamline and optimize operational processes for other organizations. As PT XYZ embraces this digitalization journey, the need for both speed and security in application development becomes increasingly critical. The process of digital transformation and app development requires not only rapid deployment to meet the dynamic demands of the market but also a strong emphasis on security. It is essential that these applications are reliable and secure, especially when handling sensitive customer data and personally identifiable information (PII). Ensuring that applications are fortified against potential threats and vulnerabilities is crucial for maintaining trust and safeguarding user information. PT XYZ must therefore implement rigorous security measures to protect both the integrity and confidentiality of the data managed by these applications, thereby reinforcing their commitment to delivering secure and dependable digital solutions.

To address the challenge of balancing rapid innovation, scalable technology, and the need to protect organizational infrastructure and, most importantly, customer data, organizations such as PT XYZ must develop a comprehensive plan to enhance their security maturity. This plan should encompass strategies for integrating cutting-edge technologies while maintaining robust security measures to safeguard sensitive information. It is crucial for PT XYZ to prioritize the creation of a security framework that not only supports the swift adoption of new technologies but also ensures resilience against emerging threats. By implementing such a plan, PT XYZ can effectively manage the complexities of modern technological advancements while ensuring the integrity and confidentiality of its data. This research is focused on implementing a DevSecOps pipeline for applications prior to their release into production or public deployment. The primary objective is to ensure that the application not only achieves rapid deployment but also maintains robust security throughout its lifecycle.

By incorporating security considerations from the very beginning of the development process, DevSecOps integrates a security perspective that addresses potential vulnerabilities early on. Moreover, the scope of DevSecOps extends beyond traditional security assessments. It also encompasses a comprehensive data security assessment to verify that the application meets necessary security maturity standards

before it is made available to the public. This holistic approach ensures that both the application and its data handling practices are thoroughly evaluated, providing a higher level of confidence in the application’s overall security posture before its launch.

1.2 Research Problem

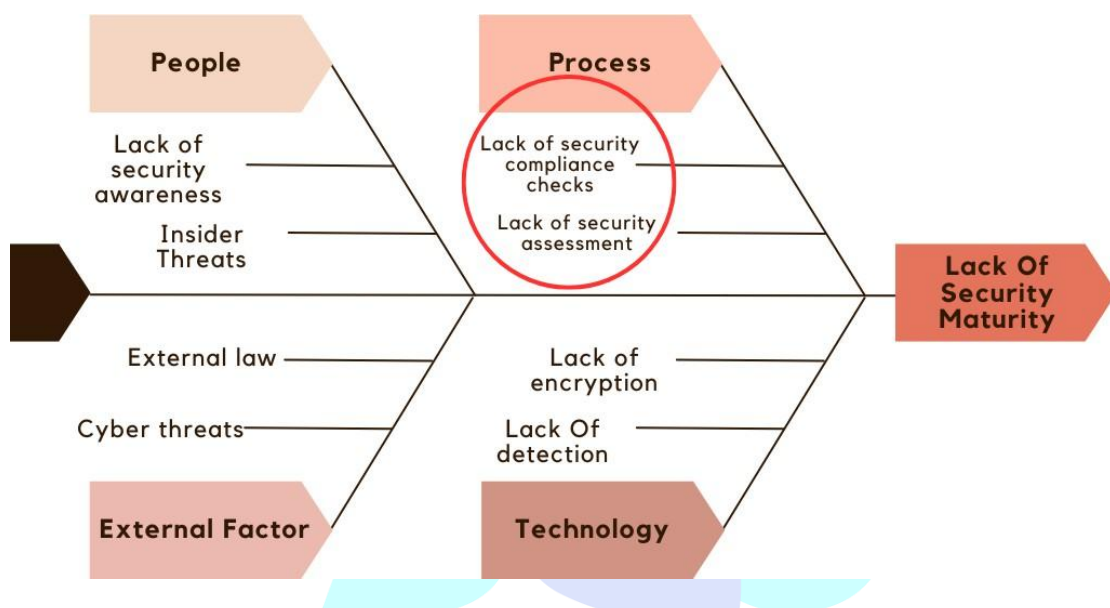


Figure 1.4: Fishbone Research Problem

The fishbone diagram that on Figure 1.4 mentioned that the lack of security maturity facing by company; one of the challenge is on the process stage that lack of security compliance checks and lack of security assessment. In addition, external issues such as adherence to external laws or government rules and the imminent presence of cyber threats present more obstacles that require the implementation of mitigation techniques for comprehensive security measures.

The security maturity in data protection is inadequate due to several issues. There is insufficient data identification and assessment to ensure proper protection. Additionally, there is a challenge in balancing the need for rapid application development with security. To address this challenge, DevSecOps is implemented to enable fast

development while ensuring security from the development stage and achieve the desired security maturity.

This research aims to enhance security maturity by conducting an analysis of DevSecOps strategies and controls within PT. XYZ each product. Then propose actionable recommendations to address gaps in security compliance and data protection, specifically in relation to UU PDP requirements.

1.3 Research Objective

The objective is to improve the security maturity of a company by addressing the gaps in the current processes, specifically in security compliance checks and security assessments. This also involves ensuring adherence to external regulations and mitigating cyber threats. The goal is to enhance data protection by implementing a DevSecOps approach, which allow for rapid application development without compromising security, ensuring that security measures are integrated from the early stages of development. Ultimately, this lead to comprehensive security practices and an elevated level of security maturity within the organization each product.

1.4 Research Question

A research question has been formulated about this topic:

1. Question #1: How can the implementation of DevSecOps framework to enhance security maturity by addressing the gaps in security compliance, assessments, and data protection, while balancing the need for rapid application development in the face of external regulations and cyber threats?
2. Question #2: What specific strategies and controls can be derived from the implementation of a DevSecOps framework to enhance security maturity in an PT XYZ Organization each product? How do these strategies comply with UU PDP requirements?

1.5 Hypothesis

A hypothesis has been formulated regarding this research:

1. Adopting a DevSecOps framework lead to measurable improvements in security maturity by bridging existing gaps in compliance, assessments, and data protection, all while supporting the swift development of applications and maintaining compliance with external regulations and managing cyber threats.
2. Strategies and controls derived from the DevSecOps framework effectively reduce risks in PT. XYZ's operations. These strategies improve and ensure the company's compliance with UU PDP requirements.

1.6 Scope and Limitation

1. The scope of this research is focused on analyzing strategies and controls derived from the DevSecOps framework to enhance security maturity in PT. XYZ each product, specifically addressing gaps in security compliance, assessments, and data protection while ensuring alignment with UU PDP requirements.
2. The limitations of this research are its specific focus on PT. XYZ products, making the findings less applicable to other organizations or industries. It is confined to strategies and controls derived from the DevSecOps framework, excluding alternative methodologies. The analysis is narrow, targeting gaps in security compliance, assessments, and data protection while overlooking other critical areas like incident response or supply chain security. Additionally, it is centered on alignment with the UU PDP, limiting its applicability to other global regulations. Broader operational, cultural, or organizational factors affecting the adoption of DevSecOps are also not addressed, potentially impacting the practicality of the proposed solutions.

1.7 Significance of Study

The research is significant for two primary reasons:

1. Enhance understanding of how DevSecOps strategies can improve security maturity and compliance within organizations like PT. XYZ.
2. Provide actionable recommendations and controls to mitigate security risks and compliance gaps, particularly related to UU PDP requirements.

1.8 Thesis Structure

The subsequent sections of this document be organized according to the following outline:

1. Chapter 1: This section provide an overview of the research, including the background, problem, objective, questions, hypotheses, scope and limitations, significance of the study, and a summary of the thesis structure.
2. Chapter 2: This section conduct a theoretical literature review, incorporating pertinent discoveries from prior research.
3. Chapter 3: This section offer a thorough explanation of the research methodologies, including the research methodology, analytical approach, assessment method, and validation procedure.
4. Chapter 4: This section presents the experimental results or findings from the research.
5. Chapter 5: This section is Conclusion.

