

# **CYBER READY: BUILDING THE NEXT GENERATION OF SECURITY PROFESSIONALS**



# Opening Context for Cybersecurity

Exploring the need for resilience in the digital era.

01

## Digital transformation rise

Organizations are rapidly adopting digital technologies to enhance operational

02

## Increasing cyber threats

With advancement comes a surge in cyber attacks, necessitating improved security measures.

03

## Importance of human capital

Resilient human capital is crucial as it plays a key role in managing cybersecurity

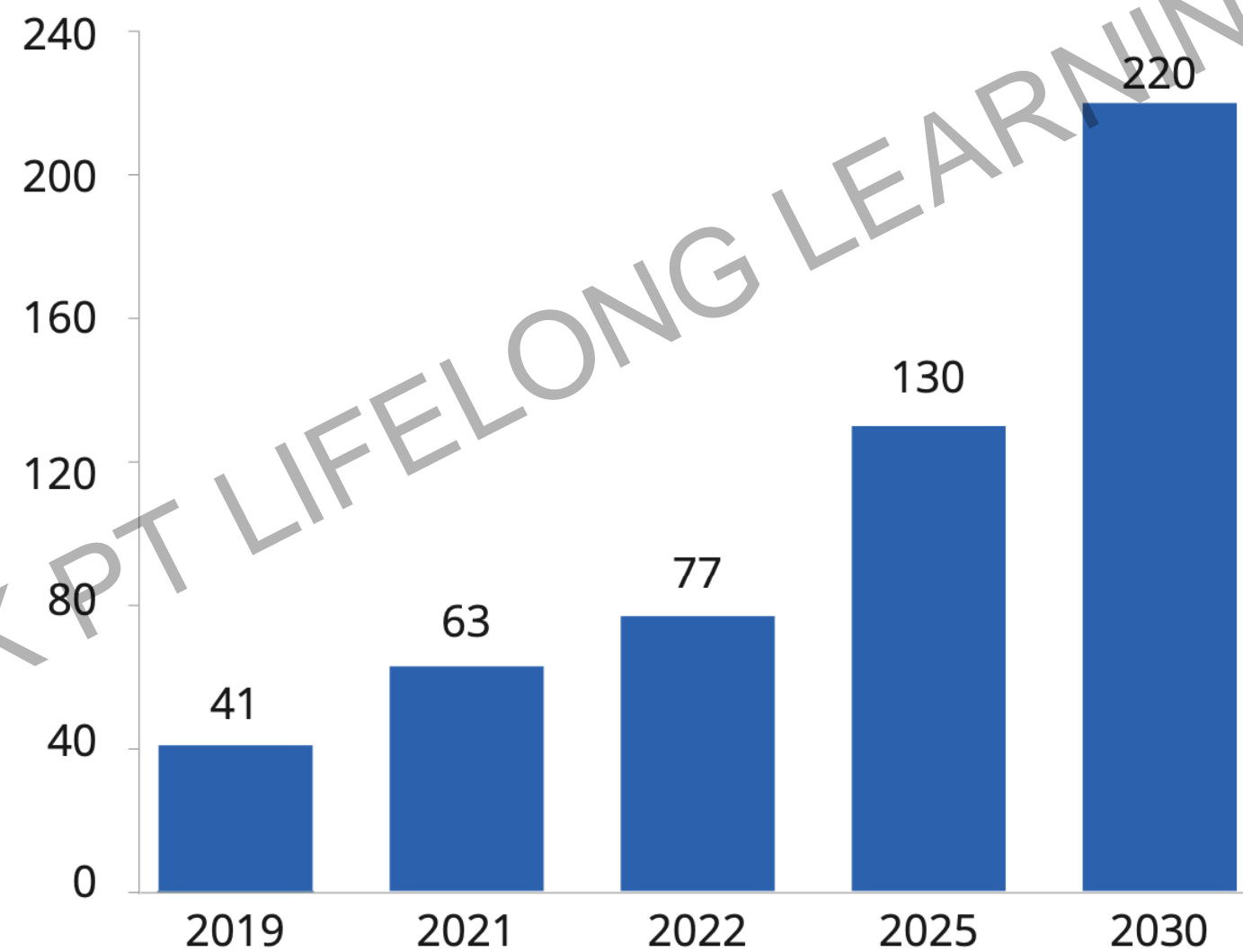


# Growth of Digital Economy

Indonesia's Prospect

## Indonesia's Digital Economy Value

GMV, in US\$ Billion

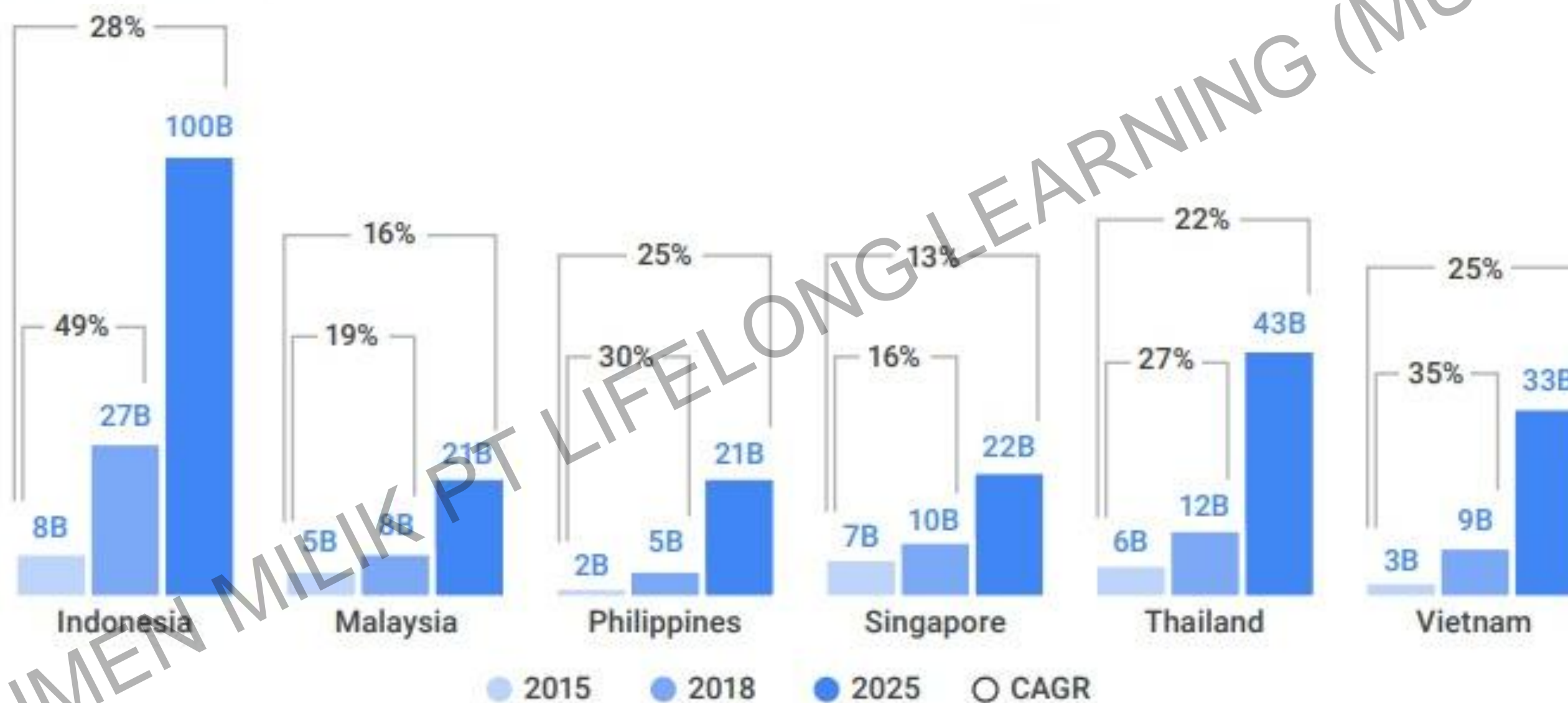


Source: Google, Temasek and Bain, e-Conomy SEA 2022



# SEA Internet Economy Market Size

Indonesia is leading the internet consumptions



# Business Impact

Indonesia's anomalies traffic statistics in 2024

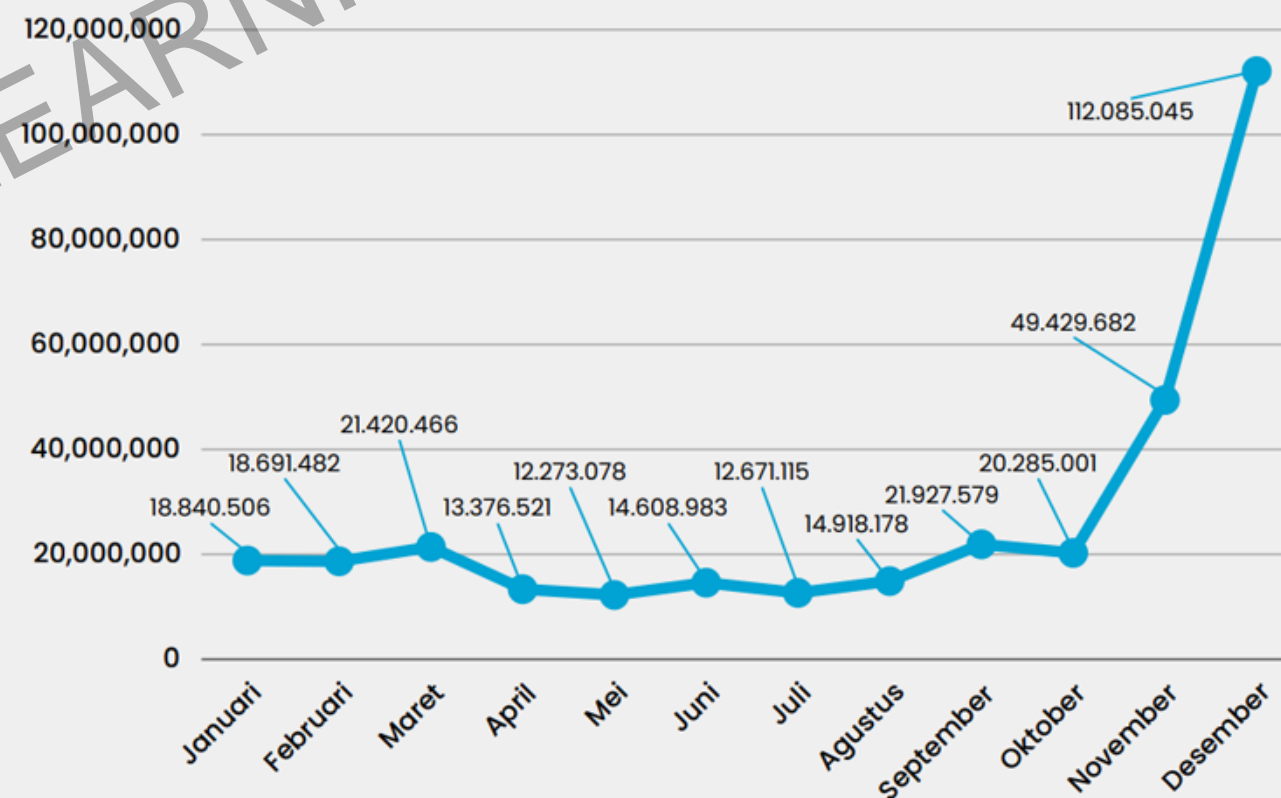
# 330.527.636

## Total Anomalous Traffic

Total anomalous traffic in Indonesia in 2024 was 330,527,636 anomalies. The highest traffic anomaly occurred in December with 112,085,045 anomalies, while the lowest anomaly occurred in May with 12,273,078 anomalies. This anomalous traffic activity can have an impact on decreasing device and network performance, theft of sensitive data, to reputation damage and decreasing trust in an organization. The following is a graph of anomalous traffic in 2024:

<https://www.bssn.go.id/wp-content/uploads/2025/02/LANSKAP-KEAMANAN-SIBER-2024-1.pdf>

The following is a graph of anomaly traffic for January-December 2024:





# Business Impact

Cyber threat can disrupt operations, lead to financial loss, damage reputation, and result in legal consequences.

## The 5 countries with the highest amount of breached accounts in 2022 were

1. RUSSIA (22.3 MILLION)
2. FRANCE (13.8 MILLION)
- 3. INDONESIA (13.2 MILLION)**
4. US (8.4 MILLION)
5. SPAIN (3.9 MILLION).

SOURCE: [HTTPS://AAG-IT.COM/THE-LATEST-CYBER-CRIME-STATISTICS/](https://aag-it.com/the-latest-cyber-crime-statistics/)

The average cost of a cyber breach in 2022 was **\$4.35 million**. It's predicted that cybercrime cost the global economy around **\$7 trillion in 2022**, and this number is expected to rise to **\$10.5 trillion by 2025**.

# Law & Regulations

Kind of Indonesia's Cybersecurity Regulations

1. **SK-275/MBU/11/2024**: Prioritas penerapan keamanan siber di BUMN, termasuk perusahaan sektor keuangan
2. **POJK No. 4/POJK.05/2021**: Kewajiban manajemen risiko TI untuk Lembaga Jasa Keuangan (LJK)
3. **Peraturan BI No. 23/6/PBI/2021**: Manajemen risiko dalam penggunaan teknologi informasi oleh Bank
4. **Undang-Undang Perlindungan Data Pribadi (UU PDP)**: Mewajibkan pengendali data melindungi informasi pribadi nasabah
5. **PP No. 71 Tahun 2019 (PP PSTE)**: Penyelenggara sistem elektronik harus menerapkan sistem pengamanan informasi



# Indonesia's Cybersecurity Talent Statistics

Current Trends and Projections



## Estimated 1,800 certified professionals

As of 2024, there are approximately 1,800 certified cybersecurity professionals in Indonesia.



## Projected demand exceeds 25,000

National demand for cybersecurity professionals is expected to exceed 25,000 by 2026.



## Sources: BSSN, Kominfo, IDC Asia Pacific

Data sourced from reputable organizations including the BSSN, Kominfo, and IDC Asia Pacific.



# The Cyber Skills Gap: A Critical Challenge

Exploring the global shortage and Indonesia's pressing upskilling needs



## Global shortage of cyber roles

There is a global deficit of approximately 3.5 million cybersecurity positions needing urgent fulfillment.



## Indonesia's urgent upskilling need

Indonesia faces a critical need to enhance workforce skills to address cybersecurity threats effectively.



## Risk of unfilled critical roles

Vacant essential cybersecurity roles lead to increased vulnerability and risk for organizations worldwide.



# What Is Cyber Readiness?

Essential Aspects of Cybersecurity Preparedness

## Cyber Readiness as a Mindset

Emphasizes the importance of a proactive approach and continuous improvement in cybersecurity awareness.

03

## Definition of Cyber Readiness

Cyber readiness refers to the state of being prepared to anticipate, withstand, and recover from cyber threats.

01

## Key Competencies Required

Essential skills include knowledge of security practices, technical skills, and awareness of cyber threats.

02



# Why Cybersecurity Skills Matter

Key challenges driving demand for cybersecurity expertise today



## Data-Driven Society Growth

Modern society relies heavily on data, increasing the value and vulnerability of information assets.



## Rising Cybercrime Threats

Cyberattack methods like ransomware and phishing are rapidly increasing in frequency and sophistication.



## Regulatory Pressure Intensifies

Growing compliance and legal requirements demand stronger cybersecurity measures across industries.

DOKUMEN MILIK PT LIFELONG LEARNING (MULTIMATICS)



# Importance for Individuals

Essential Aspects of Cybersecurity Education



## Personal Data Protection

Safeguarding personal information is crucial in preventing identity theft and privacy violations.



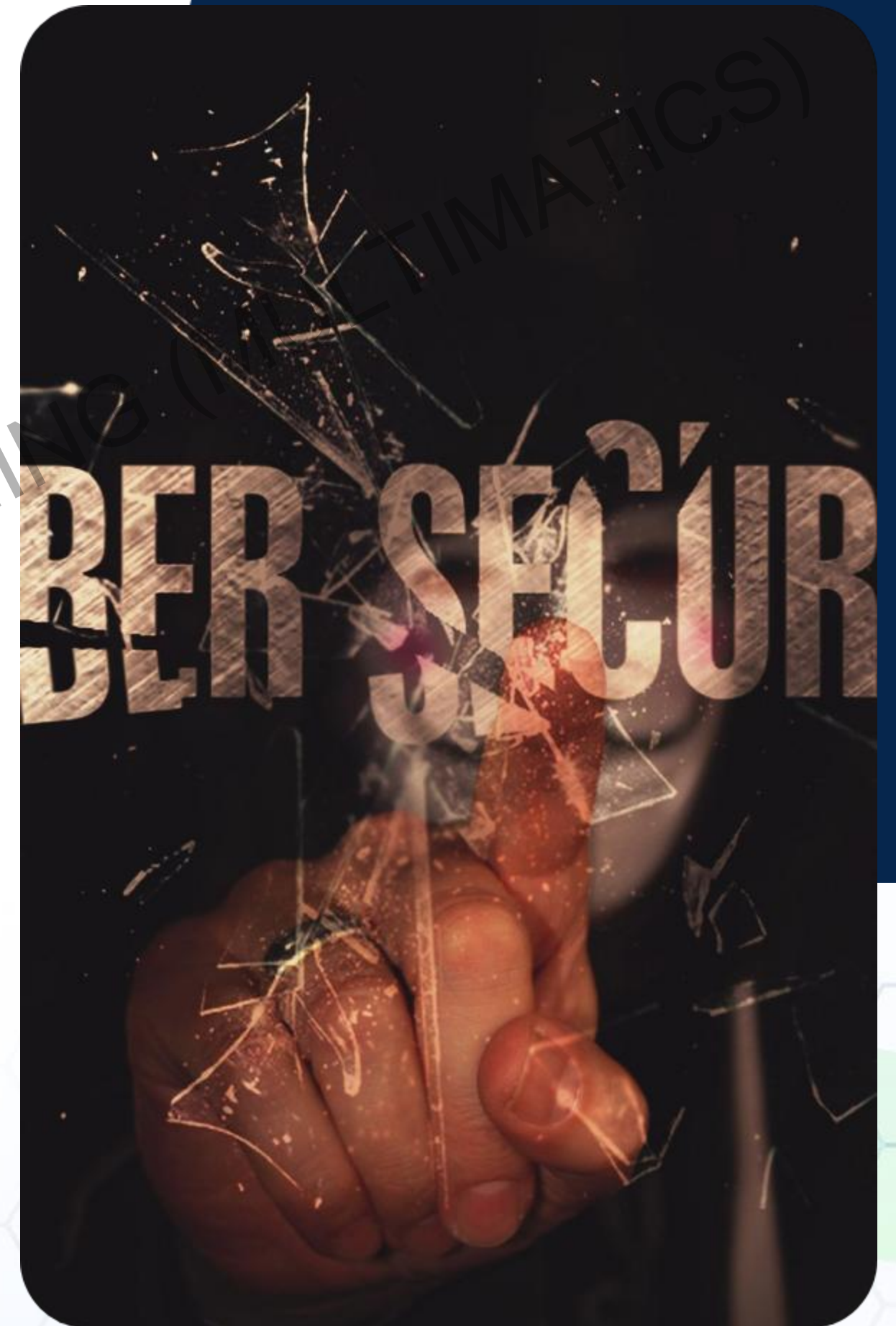
## Safe Digital Practices

Adopting secure online behaviors can significantly reduce risks associated with cyber threats.



## Foundation for Career Advancement

Mastering cybersecurity skills is vital for enhancing career prospects in today's digital job market.



# Importance of Cybersecurity for Institutions

Exploring key benefits of robust cybersecurity measures for educational institutions.



## Business Continuity

Ensures that critical operations remain uninterrupted in the face of threats.

## Customer Trust

Instills confidence among students and stakeholders through data protection.

## Regulatory Compliance

Helps institutions adhere to legal and industry standards for data security.



# Importance for Society & Nation

Critical Aspects of Cybersecurity's Role



## Defending Critical Infrastructure

Ensuring robust defenses against cyber threats to protect essential services like power and water.



## Enhancing Digital Resilience

Building systems and protocols that withstand cyber attacks and recover quickly from disruptions.



## Fostering Social Trust

Encouraging user confidence in technology through transparent and secure practices in digital interactions.

# Why We Need to Learn Cybersecurity

Addressing the Critical Skills Gap



## Shortage of Skilled Professionals

The cybersecurity field faces a severe shortage of qualified individuals, impacting organizational security.



## Rapid Technology Changes

Technology evolves at a pace that outstrips the public's awareness, making consistent education essential.



## Digital Responsibility for All

Cybersecurity is not just the job of specialists; it requires awareness from every individual in the digital space.



# Career Impact of Cyber Skills

Explore how acquiring cyber skills can significantly advance your career, boost earnings, and provide versatile job opportunities across industries.

## Boost Employability

Cyber skills increase your chances of securing jobs in a competitive market by meeting in-demand qualifications.

01

## Higher Income Potential

Professionals with cyber skills often command better salaries due to specialized knowledge and high demand.

02

## Transferable Across Industries

Cybersecurity abilities apply widely, enabling career flexibility in sectors like finance, healthcare, and technology.

03

# Real Roles in Cybersecurity

Exploring Key Career Opportunities

## 01 SOC Analyst Roles

A SOC Analyst monitors and responds to security incidents, safeguarding the organization from cyber threats.

## 02 GRC Specialist Needs

Governance, Risk, and Compliance (GRC) Specialists ensure organizations comply with laws and regulations, managing risk effectively.

## 03 Pentester Skill Set

Pentesters simulate attacks to identify vulnerabilities, requiring both technical skills and creativity in problem-solving.

## 04 Risk Manager Duties

Risk Managers analyze and mitigate potential security risks, combining analytical skills with strategic vision for the organization.

## 05 Career Path Progression

From entry-level roles to senior positions, career paths in cybersecurity include various specializations and growth opportunities.





### **Impact on All Departments**

Legal, HR, Audit, and Procurement are increasingly affected by cybersecurity risks.



### **Rise of Hybrid Roles**

The emergence of dual-hatted professionals highlights the need for cybersecurity knowledge across roles.



### **Cyber Awareness Skills**

Cybersecurity awareness is becoming an essential skill for all employees, not just IT staff.

# **Cybersecurity for Non-IT Professionals**

Understanding the impact of cybersecurity across various business functions and the importance of awareness.



# Career Opportunities in Indonesia

Exploring Key Sectors and Demands



## Key sectors hiring now

Major sectors like banking, government, telecom, and startups are actively seeking new talent.



## Increasing need in cloud security

The rise of cloud computing has created a substantial demand for cloud security professionals.



## Forensics and GRC roles

Organizations are on the lookout for professionals skilled in forensics and Governance, Risk, and Compliance (GRC).



## Demand for international certifications

Certifications such as CEH, CISSP, and CISA are increasingly sought after to enhance career prospects.

# Cyber Readiness Business Case

How Company X Enhanced Cybersecurity  
Readiness



## Incident Rate Reduction

Company X reduced incident rate by 70%, showcasing significant improvement in security.



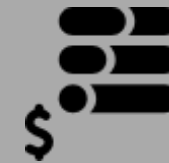
## Faster Response Time

Achieved faster response times to incidents, minimizing potential damage from attacks.



## Staff Training Initiative

Trained 100+ staff via internal academy, enhancing workforce skills in cybersecurity.



## Lower Compliance Cost

Reduced compliance costs due to improved security measures and lower incidence of breaches.



# Key Benefits of Cyber Readiness

Empowering Security Professionals

01

## Upskilled Government Auditors

Enhanced skill sets for auditors resulted in improved cybersecurity capabilities and responses to threats.

02

## Reduced Third-Party Risks

Implemented measures that significantly decreased vulnerabilities and exposure to third-party partners.

03

## Stronger Public Trust

Building credibility through transparent cybersecurity practices has fostered greater confidence among the public.

# Return on Investment (ROI)

Evaluating Investment in Cybersecurity Training

**\$50**

## Cost of Breach

Estimated average cost of a data breach.

**\$10**

## Training Cost

Annual cost of employee cybersecurity training.

**90%**

## Retention Rate

Employees retained after training.

**25%**

## Downtime Reduction

Percentage decrease in downtime due to better practices.

**\$5**

## Penalty Savings

Potential savings from avoided penalties.



# Building the Future Talent Pipeline

Strategic Objectives for Cybersecurity Workforce Development

## Foster Academia-Industry Collaboration

Promote partnerships between universities, industries, and government to align education with workforce needs.

## Develop National Cybersecurity Strategy

Create and execute a nationwide plan to address talent shortages and unify efforts across sectors.



## Expand Practical Training Programs

Implement internships, bootcamps, and mentoring initiatives to enhance hands-on cybersecurity skills.

# Empower the Future of Cybersecurity

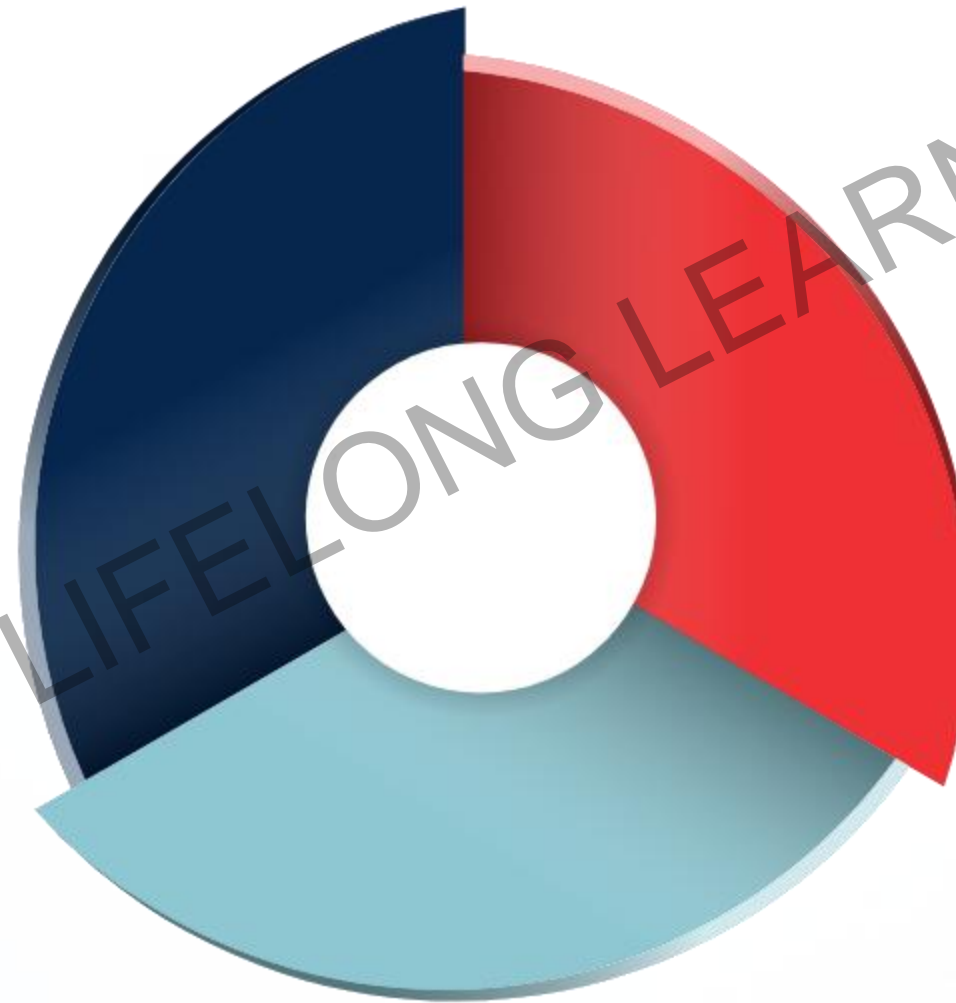
Join the Movement for Security Awareness

## Empower and Equip the Next Generation

Foster skills and knowledge to prepare future security professionals.

## Be Part of the Cyber Defense Ecosystem

Collaborate with organizations and communities to strengthen defenses.



## Prioritize Security Awareness and Learning

Encourage ongoing education in cybersecurity principles and practices.



# THANK YOU

**MULTIMATICS**

AXA Tower 37<sup>th</sup> Floor, Jl.Prof.Dr. Satrio Kav. 18, Kuningan City, Jakarta Selatan  
T: 021-30056123 | F: 021-30056124 | 087781233050 | [www.multimatics.co.id](http://www.multimatics.co.id)



multimatics\_ID



multimatics



multimatics ID



multimaticsID