KISA Cybersecurity Education and Training Status and Plans Report

---

1. Introduction

Cybersecurity education and training is no longer limited to the acquisition of technical skills. It increasingly requires convergent knowledge that spans information technology, software, telecommunications, and emerging digital technologies. Beyond the traditional security industry, demand for cybersecurity professionals has expanded across multiple sectors, including finance, manufacturing, healthcare, and the public domain.

This report analyzes the current status of KISA's cybersecurity education and training initiatives and outlines future plans aimed at strengthening national cybersecurity capabilities and building a sustainable professional ecosystem.

---

2. Current Status of Cybersecurity Education and Training

2.1 Changing Industry Environment

- Cybersecurity has evolved into an integrated discipline that combines IT, software, cloud, and AI expertise.
- Professionals are entering diverse industries where tailored security skills are required, such as financial services, industrial operations, and healthcare.

2.2 Need for Workforce Development and Competency Building

- Cybersecurity personnel require both technical expertise and sector-specific knowledge.
- Current education and training systems are not fully aligned with industry demand, creating imbalances in workforce supply.
- Competencies in incident response, security governance, and hands-on operational skills are particularly critical.

---

3. Analysis of KISA's Training Strategies

3.1 Competency-Based Education

- Transition from theory-focused courses to practice-oriented programs such as cyberattack and defense simulations, incident response exercises, and SOC operations.
- Alignment of curricula with global frameworks such as the NICE Framework and the ECSF to ensure standardization.

3.2 Demand-Driven Workforce Development

- Development of specialized courses tailored to industry needs, such as financial security, medical security, and OT/ICS protection.
- Expansion of training programs designed for SMEs and public institutions with limited resources.

3.3 Continuous Competency Assessment

- Implementation of ongoing assessment and feedback systems instead of one-time evaluations.
- Integration of certification, capability validation, and simulation-based evaluation to build a comprehensive verification system.

---

4. Future Plans

4.1 Expansion of Training Programs

- Broaden the scope from basic awareness training to advanced incident response simulations.
- Provide both conversion programs for non-specialists and advanced courses for experienced professionals.

4.2 Strengthening Global Collaboration

- Establish joint programs with international organizations to train globally competitive experts.
- Incorporate internationally recognized certification pathways into KISA training.

4.3 Building a Cybersecurity Training Ecosystem

- Develop a collaborative network that connects public, private, and academic stakeholders.
- Ensure that training outcomes directly contribute to industry needs and national security policies.

---

5. Conclusion

KISA’s cybersecurity education and training initiatives play a crucial role in strengthening national security capacity and fostering a resilient workforce ecosystem. As cyber threats intensify and global competition rises, training must focus on practical, demand-oriented, and globally integrated approaches. Through these efforts, Korea can ensure a continuous pipeline of professionals while raising the overall level of national cybersecurity readiness.

Would you like me to **expand this into a more detailed report with quantitative data** (e.g., annual training participants, budget, outcomes) extracted directly from the slides, or should I keep it at this strategic summary level?