Construction and Practice of a Modular Hybrid Task-Driven Teaching System Based on the Security Protection Chain

Jiaokun Shi*, Hui Ke

School of Artificial Intelligence, Chongqing Vocational College of Safety Technology, Wanzhou District, Chongqing, 404020, China

*Corresponding's email: 1973760696@qq.com

Abstract. With the rapid advancement of information technology, information security has become a critical safeguard for national security and enterprise operations. However, information security programs in higher vocational colleges commonly suffer from several core issues, including the disconnect between theory and practice, outdated curriculum content, and insufficient job-readiness of graduates. To address these challenges, this study takes the course Information Security Product Configuration and Application as its research subject. Grounded in the engineering logic of the security protection chain, the course is restructured into five stages comprising eight modules: perimeter protection, threat detection, security auditing, unified management, and comprehensive practical exercises. A three-phase blended teaching model is established, encompassing pre-class online self-study, in-class offline hands-on practice, and post-class online consolidation, with an in-class pedagogical approach of "practice first, instruct next, practice again." Quasi-experimental research demonstrates that the proposed system yields significant improvements in students' knowledge acquisition, operational proficiency, and comprehensive occupational competency, offering a practical reference for curriculum reform in higher vocational information security education.

Keywords: vocational education; modular teaching; blended learning; task-driven instruction; information security education; competency-based education

1 Introduction

The digital economy is profoundly reshaping the global industrial landscape. Information security has evolved from a single technical defense domain into a foundational force underpinning national strategic security and the high-quality development of the digital economy. According to the China Cybersecurity Industry Alliance's Analysis Report on China's Cybersecurity Market and Enterprise Competitiveness (2024), China's cybersecurity market has surpassed CNY 200 billion, with a compound annual growth rate projected to remain above 15% over the

Z. Ge et al. (eds.), *Proceedings of the 2026 6th International Conference on Education, Information Management and Service Science (EIMSS 2026)*, Atlantis Highlights in Computer Sciences 25,
https://doi.org/10.2991/978-94-6239-766-8_44

next five years, driving exponential demand for highly skilled information security professionals.

However, a pronounced structural gap exists on the talent supply side. Graduates of higher vocational information security programs demonstrate a notable shortfall in occupational competency relative to enterprise requirements, manifesting across three dimensions: (1) curriculum content emphasizes theoretical instruction, leaving students without practical operational experience in real-product environments; (2) existing courses predominantly offer isolated single-product training, preventing students from understanding the coordinated logic of multi-product security systems; and (3) textbook content lags behind industry developments, with device models and deployment scenarios seriously misaligned with mainstream practice.

To address these problems, this study uses the course Information Security Product Configuration and Application as its vehicle. We propose restructuring the curriculum around the engineering logic of the security protection chain, and combining this with a three-phase blended teaching structure—pre-class online self-study, in-class offline hands-on practice, and post-class online consolidation—while introducing an in-class "practice first, instruct next, practice again" pedagogy. The resulting modular hybrid task-driven teaching system is empirically validated through a quasi-experimental study.

2 Theoretical Foundations and Literature Review

2.1 Competency-Based Education (CBE)

CBE theory advocates replacing knowledge points with observable, measurable professional competencies as the fundamental unit of curriculum design [1]. The theory holds that the ultimate goal of vocational education is to enable learners to perform real work tasks in specific occupational contexts. In the information security product domain, occupational competencies can be operationalized as engineering capabilities including NGFW policy configuration, WAF rule tuning, IDS/IPS linkage response, vulnerability report interpretation, log correlation auditing, and security solution design—providing a theoretical basis for phased curriculum construction along the protection chain logic.

2.2 Task-Based Learning (TBL)

Task-Based Learning organizes learning activities within authentic or simulated task contexts with clear objectives, allowing learners to construct knowledge and develop skills through task completion [2]. Nunan (2004) notes that TBL's effectiveness lies in activating learners' intrinsic motivation and promoting contextualized knowledge transfer. This study treats authentic enterprise engineering tasks—such as NGFW policy configuration, WAF attack protection, and comparative IPS/IDS deployment—as the basic organizational units of instruction, replacing the traditional knowledge-point-centered lecture model.

2.3 Blended Learning Theory

Blended learning organically integrates face-to-face classroom instruction with online digital learning [3]. Graham (2006) emphasizes the complementary strengths of both modes rather than simple superimposition; Picciano (2009) further proposes a multimodal blended model [4]. In vocational skill development contexts, online platforms enable front-loaded pre-learning of product knowledge and fragmented knowledge accumulation, while offline classrooms focus on equipment operation training and real-time instructor guidance, with a clear division of labor and mutual reinforcement between the two.

2.4 Constructivist Learning Theory

Constructivism emphasizes that learners construct knowledge through active exploration and experiential reflection [5]. Piaget's cognitive conflict theory posits that learning motivation is strongest—and knowledge reconstruction deepest—when learners encounter problems that cannot be explained by their existing schemas. The "practice first" component of this study's in-class pedagogy deliberately functions as a cognitive conflict activation mechanism: requiring students to operate before receiving complete instruction generates genuine operational confusion, creating a state of high demand for subsequent explanatory content and thus improving absorption efficiency.

2.5 Gaps in Existing Research

In terms of domestic and international research, scholars have conducted multi-dimensional explorations centered on cyberspace security curriculum reform and the integration of industry and education. At the pedagogical level, Yang (2024) demonstrated that task-driven teaching effectively enhances classroom efficacy [6]; Zhu (2024) argued that real-world, scenario-oriented practical teaching drives the transition from traditional knowledge-verification to hands-on, combat-ready capability cultivation [7]; and Zhang (2024) validated that competition-driven models offer a novel pathway for cybersecurity educational reform [8]. Together, these three studies reflect a clear reform trend characterized by an "emphasis on practice, focus on application, and promotion of capability."At the level of industry-education integration, Gong (2024) constructed a performance evaluation model based on coupling coordination theory [9]; Tran (2016) demonstrated the critical role of university-enterprise collaboration in improving graduate employability [10]; and Yu et al. (2025) systematically analyzed the constraints, mechanisms, and strategies facing this integration [11]. These insights collectively indicate that the insufficient depth of industry-education integration remains the core bottleneck constraining the quality of talent cultivation.Regarding the construction of practical teaching frameworks, Bendler and Felderer (2023) developed a cybersecurity job competency model [12]; Sánchez et al. (2026) proposed a practical cyber range training and certification system aligned with the ECSF framework [13]; and Ismail et al. (2024)

provided a systematic literature review on the key elements of cybersecurity curriculum design [14]. These three works echo a practical teaching reform philosophy defined by "demand orientation, combat readiness driving, and systematic integration."

These studies collectively reveal a consistent trend toward practice-oriented, application-driven, and competency-enhanced cybersecurity education reform, emphasizing task-driven pedagogy, scenario-based instruction, and competition-enabled learning, while highlighting the growing importance of industry–education integration and systematic practical teaching frameworks. However, three major research gaps remain. First, existing studies lack an integrated curriculum design grounded in the systemic engineering logic of the cybersecurity defense chain. Second, most works fail to systematically articulate a complete instructional cycle following a "practice-first, instruction-after, re-practice-enhancement" paradigm. Third, empirical validation remains limited, with a shortage of quantitative pre- and post-test comparisons to rigorously evaluate teaching effectiveness. These gaps collectively define the research motivation of this study.

3 Analysis of Problems in Existing Higher Vocational Information Security Curricula

3.1 Isolated Single-Product Training and Lack of Systemic Logic

Through systematic review of information security curricula at 17 higher vocational colleges in Chongqing, supplemented by field research with graduates from three cohorts and more than ten enterprises, we find that existing courses universally use single-product operation as the instructional unit, with no logical connection between modules. Students studying NGFW are unaware of its coordination with IPS and WAF; students studying IDS do not understand its linkage with OSMS platforms. Approximately 68.7% of surveyed enterprises reported that graduates can operate individual devices but cannot design comprehensive protection solutions—reflecting a capability gap in transitioning from single-product operation to system-level design.

3.2 Excessive Theoretical Hours and Insufficient Practical Opportunity

Survey results indicate that practical laboratory hours in current higher vocational information security courses remain low, and experiment content is predominantly verification-based with predetermined steps and preset answers, lacking exploration and integration. Students' cumulative hands-on configuration training time with real security products (e.g., NGFW, IDS, WAF) is generally under 15 hours—far below the 40–60-hour practical benchmark typically required by enterprises for pre-employment training. Approximately 73.5% of surveyed enterprises reported that applicants cannot independently complete basic job operations.

3.3 Traditional Lecture-Then-Practice Model and Low Efficiency

Existing courses universally adopt a linear logic of completing lecture before arranging practice. Students receive principle-based instruction before any hands-on exposure, lacking the drive of real operational problems; their sense of knowledge need is weak and understanding remains abstract. Constructivist learning theory demonstrates that activating cognitive conflict before offering explanations yields far superior learning outcomes compared to front-loading knowledge then verifying through practice.

4 Overall Design of the Teaching System

4.1 Design Philosophy and Framework

The teaching system proposed in this study takes the engineering logic of the security protection chain as the curricular backbone, uses occupational competency as the design starting point, and adopts the three-phase blended teaching structure as its organizational framework. The "practice first, instruct next, practice again" pedagogy serves as the core in-class mechanism, forming a closed-loop system: occupational competency analysis → chain-based curriculum design → three-phase blended teaching implementation → multi-dimensional support and evaluation feedback. The overall design follows the backward design principle of Outcome-Based Education (OBE), working from expected learning outcomes to derive the instructional activity design. Figure 1 illustrates the complete framework.

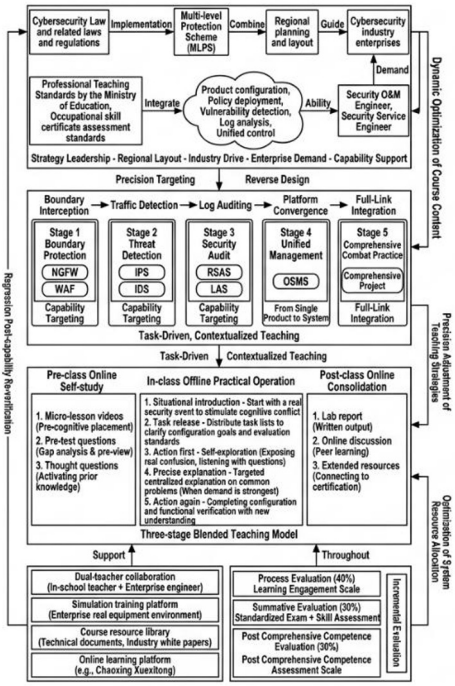

Fig. 1. Framework of the Modular Hybrid Task-Driven Teaching System Based on Occupational Competency

4.2 Five-Stage, Eight-Module Curriculum Architecture

Based on the complete workflow of information security engineer positions, the course is restructured into five protection stages and eight instructional modules. Each stage serves a clearly defined engineering role within the protection chain, with inherent interconnection and progressive logic between modules. The overall flow proceeds from the network perimeter through threat detection and security auditing, rising to a unified management platform, and finally achieving full-chain integration in comprehensive practical exercises.

The perimeter protection stage deploys NGFW and WAF to establish access control barriers at the network and application layers respectively. The threat detection stage combines IPS and IDS into a complementary configuration of in-line blocking and out-of-band monitoring. The security auditing stage features RSAS and LAS representing proactive prevention and post-hoc traceability perspectives. The unified management stage's OSMS serves as the convergence point for the preceding six modules, enabling students to understand how individual product capabilities transform into systemic capability. The comprehensive practical stage requires students to complete a full engineering project from requirements analysis to documentation delivery, achieving the critical transition from knowing how to operate to knowing how to design.

5 Three-Phase Blended Teaching Model and Pedagogy

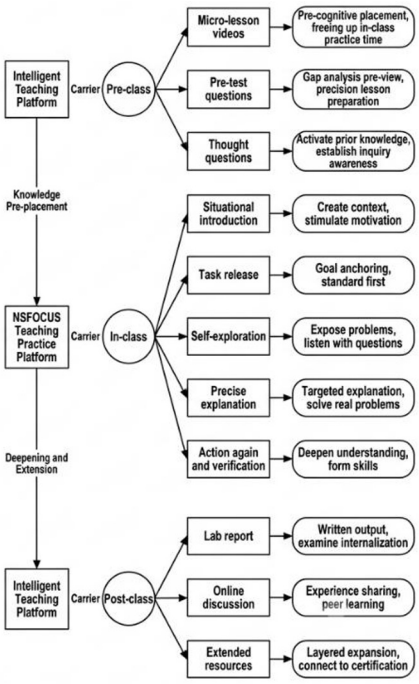

Fig. 2. Three-Phase Blended Teaching Structure Design

Each module adopts a three-phase blended teaching structure: pre-class online self-study → in-class offline hands-on practice → post-class online consolidation (Figure 2). The pre-class phase front-loads cognitive content to release maximum in-class time for practice; the in-class phase centers on skill formation and complex problem-solving; the post-class phase verifies learning internalization and provides differentiated extension resources.

5.1 Pre-class Online Self-study Design

The pre-class phase comprises three components: micro-lecture videos, pre-assessment questions, and reflection prompts. Micro-lecture videos front-load product cognitive content—including product white papers, operating principles, technical background, and typical application scenarios—onto a smart teaching platform, enabling students to self-study during fragmented time. Pre-assessment questions include multiple-choice and true/false items to gauge students' knowledge baseline and guide instructors in targeted lesson preparation. Reflection prompts serve as open-ended questions to encourage students to enter class already thinking, preparing them for the "practice first" component of the in-class sequence.

5.2 In-class Offline Hands-on Practice

The in-class component's central concept is "practice first, instruct next, practice again": by moving the activation of cognitive conflict to before knowledge input, the instructional explanation occurs at the moment of greatest student need—facilitating the transition from passive knowledge reception to active knowledge construction. The in-class component comprises five steps:

Step 1 — Contextual Introduction. Instruction begins with a real security incident or representative enterprise case to stimulate student interest and establish the learning task. For example, in the NGFW module, a real incident of internal data leakage caused by misconfigured access control policies is used as the case entry point.

Step 2 — Task Release. A task sheet is distributed specifying the product configuration objectives, verification standards, and scoring criteria, ensuring that students know the required completion level before operating and enabling self-assessment and peer assessment.

Step 3 — Independent Exploration. Students independently operate according to the lab manual. This is the core component of the "practice first" philosophy; its purpose is to develop students' task comprehension, practical operation, and autonomous problem-solving abilities—and crucially, to bring genuine operational confusion into the next instructional step. Cognitive conflict theory indicates that students' need for knowledge is most acute when they are experiencing cognitive confusion, and absorption efficiency far exceeds baseline.

Step 4 — Targeted Instruction. Based on classroom observation and pre-assessment data, the instructor provides concentrated instruction targeting common problems identified among students, while organizing group discussion for other issues. The key is that students listen with specific problems in mind, enabling precise alignment between explanation and confusion.

Step 5 — Repeated Practice and Verification. Armed with new understanding, students revisit the experiment to complete the full configuration operation and functional verification. Instructors circulate to provide individual coaching. The session concludes with a collective review summarizing core knowledge points and operational principles, followed by post-class task assignment.

5.3 Post-class Online Consolidation Design

The post-class phase achieves learning internalization and differentiated extension through three components: lab report submission, online topic discussion via the smart teaching platform, and extension resources. Structured lab reports require students to document experimental topology, device parameters, procedures, results, and reflections. Platform-based discussion forums facilitate peer learning and experience sharing. Extension resources—including vendor product videos, technical documentation, and certification question banks—meet students' needs for extended learning.

6 Experimental Research Design and Results Analysis

6.1 Research Design

This study selected two parallel classes from the 2025 cohort of the Information Security Technology Application program as the experimental subjects. One class (n = 37) was assigned as the experimental group and implemented the proposed teaching approach, while the other class (n = 35) served as the control group and adopted the traditional instructional sequence of "theory first, practice later." The experiment lasted one academic semester, and both groups received identical instructional content.

To comprehensively evaluate the instructional effectiveness, a four-dimensional evaluation framework was established. The first dimension, knowledge acquisition, was assessed using a standardized written examination administered before and after the intervention (Cronbach's $\alpha = 0.87$). The second dimension, operational skill mastery, was evaluated through practical task performance based on occupational competency behavioral indicators, with an inter-rater reliability coefficient of $r = 0.91$. The third dimension, comprehensive occupational competency, was measured using a task-based assessment rubric jointly developed by university faculty and enterprise experts, covering mastery of six categories of cybersecurity products and technical report writing. The fourth dimension, learning engagement, was evaluated using learning analytics collected from the smart teaching platform, including course resource access (40%), topic participation (10%), and task completion (50%).

6.2 Experimental Results

The pre-test results indicated no significant difference between the experimental and control groups in baseline knowledge performance ($t = 0.73$, $p = 0.47$), confirming the comparability of the two groups before the intervention.

As shown in Table 1, the post-test results demonstrated that, in the knowledge acquisition dimension, the experimental group achieved a significantly higher mean score ($M = 77.9$, $SD = 7.2$) than the control group ($M = 72.4$, $SD = 8.6$), $t(70) = 2.96$, $p < 0.01$, with Cohen's $d = 0.70$, indicating a medium effect size.

For the operational skills dimension, the practical examination pass rate of the experimental group reached 82%, representing an improvement of 15 percentage points over the control group (67%). Although the difference did not reach statistical significance ($p > 0.05$), it indicates a noticeable improvement in practical performance.

Regarding comprehensive occupational competency, the experimental group's post-test mean score (80.1) was significantly higher than that of the control group (71.8), with $p < 0.01$ and an eta-squared (η^2) value of 0.11, indicating a moderate instructional effect. Compared with the pre-test score, the experimental group improved by 21.5 points.

For the learning engagement dimension, the experimental group achieved a composite score of 86.7, exceeding the control group's score of 76.5 by 10.2 points,

representing a relative improvement of approximately 13.3%. In addition, the experimental group's post-test performance in knowledge acquisition, comprehensive occupational competency, and learning engagement was significantly higher than its corresponding pre-test performance ($p < 0.001$).

It is also noteworthy that, after course completion, both groups participated in the institutional course evaluation. The experimental group achieved an overall student satisfaction rate of 97.3%, approximately 8 percentage points higher than that of the control group. Furthermore, institutional teaching supervisors reported that students in the experimental group demonstrated a clearer overall cognitive understanding of the course content. The instructional sequence of "practice first, instruction afterward" enabled subsequent targeted explanations to be more focused and effective.

Table 1. Comparison of teaching outcomes between experimental and control groups ($n_{exp} = 37$, $n_{ctrl} = 35$)

Assessment Dimension	Indicator	Exp. Group (Pre-test)	Exp. Group (Post-test)	Ctrl. Group (Post-test)	Improvement (Exp. Group)
Knowledge acquisition	Standardized theory test (mean score)	61.3	77.9	72.4	16.6
Operational skills	Practical assessment pass rate	48%	82%	67%	34%
Comprehensive occupational competency	Occupational competency score	58.6	80.1	71.8	21.5
Learning engagement	Composite score: resource access (40%), topic participation (10%), task completion (50%)	62.1	86.7	76.5	24.6

Note: *The post-test scores of the experimental group across all dimensions were higher than their corresponding pre-test scores, with improvements in knowledge acquisition, comprehensive occupational competency, and learning engagement reaching statistical significance ($p < 0.001$). In the post-test comparison between the experimental and control groups, the differences in knowledge acquisition and comprehensive occupational competency were statistically significant ($p < 0.01$). Although the practical examination pass rate improved by 15 percentage points, the difference did not reach statistical significance ($p > 0.05$).*

6.3 Results Analysis

These results show high consistency with prior research and may be attributed to three factors: (1) structuring the curriculum around engineering chain logic enables organic integration of knowledge within authentic work contexts, facilitating holistic understanding; (2) the "practice first, instruct next, practice again" mechanism causes instructional explanation to occur at the moment of greatest cognitive demand, with absorption efficiency exceeding conventional instruction; and (3) contrastive task design strengthens conceptual differentiation and transfer capacity through comparative knowledge activation.

7 Conclusion and Future Work

This study proposed and empirically validated a modular hybrid task-driven teaching system based on the engineering logic of the security protection chain. By constructing a five-stage, eight-module curriculum architecture, the fragmented structure of isolated single-product training was broken, effectively addressing the capability gap in transitioning from single-product operation to system-level design. Through rational allocation of learning activities—front-loading cognitive content and concentrating class time on hands-on practice—efficiency of knowledge transmission and depth of skill development were both achieved. Through the in-class "practice first, instruct next, practice again" model, problem-oriented feedback supplemented theoretical instruction to maximize instructional effectiveness.

Future work will: (1) extend validation across multiple courses and disciplines to improve external validity; (2) conduct longitudinal tracking studies to examine the system's sustained impact on students' occupational adaptation after employment; and (3) explore the integration of AI-assisted personalized learning path recommendation with the course to further improve instructional precision.

Acknowledgments

This work was supported by the 2024 Institutional Education and Teaching Reform Research Project of Chongqing Vocational College of Safety Technology (Grant No. AQJG24-06).

References

1. William G. Spady. 1994. Outcome-Based Education: Critical Issues and Answers. American Association of School Administrators, Arlington, VA, 1–28.
2. David Nunan. 2004. Task-Based Language Teaching. Cambridge University Press, Cambridge, UK, 11–37.
3. Charles R. Graham. 2006. Blended learning systems: definition, current trends, and future directions. In The Handbook of Blended Learning, Curtis J. Bonk and Charles R. Graham (Eds.). Pfeiffer, San Francisco, CA, 3–21.
4. Anthony G. Picciano. 2009. Blending with purpose: the multimodal model. Journal of Asynchronous Learning Networks 13, 1 (2009), 7 – 18. https://doi.org/10.24059/olj.v13i1.1673
5. Jean Piaget. 2001. The Psychology of Intelligence. Translated by Malcolm Piercy and D. E. Berlyne. Routledge, London, UK, 3–26.
6. Shasha Yang, Wenjing Ma, and Jianjun Wu, et al. 2024. Teaching reform of introduction to cyberspace security based on task-driven approach. Computer Education 8 (2024), 60–64. https://doi.org/10.16512/j.cnki.jsjjy.2024.08.014 (in Chinese)
7. Yi Zhang, Xiaodong Zhu, and Yuanyuan Ma, et al. 2024. Practice-oriented teaching reform for cyberspace security majors driven by real-world scenarios. Computer Education 11 (2024), 187–191. https://doi.org/10.16512/j.cnki.jsjjy.2024.11.043 (in Chinese)

8. Sizheng Zhu, Shanshan Wang, and Ye Xu, et al. 2024. Exploration of competition-driven teaching reform in cybersecurity education. Advances in Education 14, 12 (2024), 51–58. https://doi.org/10.12677/ae.2024.14122231 (in Chinese)
9. Xianwen Gong. 2024. Performance evaluation of industry-education integration in higher education from the perspective of coupling coordination — an empirical study based on Chongqing. PLOS ONE 19, 9 (2024), e0308572. https://doi.org/10.1371/journal.pone.0308572
10. Thi Tuyet Tran. 2016. Enhancing graduate employability and the need for university-enterprise collaboration. Journal of Teaching and Learning for Graduate Employability 7, 1 (2016), 58–71. https://doi.org/10.21153/jtlge2016vol7no1art598
11. Bo Yu, Ruipu Li, Siyuan Zhang, Peng Mao, Chun Xu, Jing Shi, and Gang Wu. 2025. Constraints, mechanisms, and strategies for industry-education integration in vocational education: An empirical study. PLOS ONE 20, 12 (2025), e0339158. https://doi.org/10.1371/journal.pone.0339158
12. Daniel Bendler and Michael Felderer. 2023. Competency models for information security and cybersecurity professionals: Analysis of existing work and a new model. ACM Transactions on Computing Education 23, 2, Article 25 (June 2023), 33 pages. https://doi.org/10.1145/3573205
13. Julia Sánchez, Alan Briones, Sara Ricci, Jakub Čegan, Argyro Chatzopoulou, Yianna Danidou, Andreas Menegatos, and Guiomar Corral. 2026. A framework for designing and certifying ECSF-aligned cybersecurity training through cyber ranges and virtual learning environments. International Journal of Information Security 25, 2, Article 46 (2026). https://doi.org/10.1007/s10207-025-01202-0
14. Muhusina Ismail, Nisha Thorakkattu Madathil, Meera Alalawi, Saed Alrabaee, Mohammad Al Bataineh, Suhib Melhem, and Djedjiga Mouheb. 2024. Cybersecurity activities for education and curriculum design: A survey. Computers in Human Behavior Reports 16 (Dec. 2024), Article 100501. https://doi.org/10.1016/j.chbr.2024.100501