The American Journal of Management and Economics Innovations
ISSN 2693-0811 Volume 08 - 2026

Specifics of Effective Selection and Training of Security Personnel in Large Companies

Maksym Ivanov
Kyiv University of Tourism, Economics and Law. Organization Management. Specialist. Dublin, IL, USA.

Received: 28 Feb 2026 | Received Revised Version: 12 Mar 2026 | Accepted: 19 Mar 2026 | Published: 30 Apr 2026

Volume 08 Issue 01 2026 |

Abstract

The study is dedicated to the systematization and analysis of existing approaches to the selection and training of security service personnel. The aim of the research is to examine the specific characteristics of effective recruitment and subsequent training of security staff in large corporations. The methodological framework comprises analysis and synthesis of recent scientific publications on psychophysiological diagnostics of candidates, evaluation of the predictive validity of selection techniques, and the integration of immersive VR/AR technologies and digital twins into training programs. As a result, a synergistic model is proposed that combines multilevel psychodiagnostic profiles with an architecture of adaptive training programs, enabling the creation of personalized development trajectories for employees and enhancing their resilience to stressful and unexpected situations. The scientific contribution lies in the substantiation of a competency-based synergistic model that links candidates' psychodiagnostic data with adaptive learning modules based on digital twins and VR technologies. The practical significance of the findings consists in their applicability for security managers, human resources directors, and specialists responsible for the development of corporate security systems in large organizations.

Keywords: corporate security; personnel selection; personnel training; competency-based approach; psychodiagnostics; insider threats; VR technologies in training; adaptive learning; human resource management; security services.

Cite This Article: Ivanov, M. (2026). Specifics of Effective Selection and Training of Security Personnel in Large Companies. The American Journal of Management and Economics Innovations, 8(04), 60–66. Retrieved from https://theamericanjournals.com/index.php/tajmei/article/view/7983

Introduction

The modern business environment is characterized by the continuous escalation and hybridization of threats confronting large corporations. Possessing concentrated tangible, financial, and informational assets, such organizations become priority targets for a wide range of destructive measures — from traditional physical and engineering assaults to sophisticated cyberattacks and targeted social engineering operations. Insider threats pose a particular danger, arising when risks originate from the organizations' own employees. According to the IBM Cost of a Data Breach Report 2023, the average cost of a data breach incident resulting from intentional insider actions amounts to USD 4.90 million, emphasizing the critical importance of rigorous selection and monitoring of security personnel [1]. Furthermore, it is projected that by 2025 up to 50 percent of all cyber incidents in large corporations will be attributable to human factors — whether through errors or deliberate misconduct by employees [2]. Under such circumstances, the reliability of a corporate security system depends not only on its technical infrastructure

but also on the professional competence, loyalty, and stress resilience of security specialists [3, 4].

Despite numerous studies dedicated to individual processes of security personnel management, the literature reveals a lack of a comprehensive methodological approach. Recruitment practices are typically confined to verifying formal criteria and administering basic psychodiagnostic assessments, while training programs remain standardized and do not account for employees' individual psychological characteristics or the evolving threat landscape. Consequently, a disparity arises between the in-depth candidate evaluation at the selection stage and the subsequent framework of professional development.

The objective of the study is to examine the distinctive features of effective personnel selection and subsequent training of security service staff in large corporations.

The scientific novelty consists in substantiating a synergistic competency model that links candidates' psychodiagnostic data with adaptive learning modules based on digital twins and virtual reality technologies.

The author's hypothesis holds that the implementation of a model incorporating in-depth psychodiagnostics at the selection stage and immersive training not only enhances individual professional performance of security personnel but also cultivates their predictive competencies for effective counteraction against nonlinear and unconventional threats, thereby substantially reducing security risks for large corporations.

Materials and Methods

In recent years, organizations have increasingly confronted the need not only for effective recruitment but also for ongoing training of their security teams amid ever-evolving cyber threats and significant economic risks. IBM and Gartner analytical reports highlight escalating costs associated with data breaches and a growing tendency to integrate emerging technologies into security processes. According to the Cost of a Data Breach Report 2023, the average incident cost has risen year on year, prompting large enterprises to revise hiring criteria to encompass both technical and behavioral competencies [1]. Likewise, Gartner forecasts that by 2024, priority will be given to professional's adept at using AI tools, adapting to virtual learning environments, and possessing skills for preemptive responses to hybrid threats [2].

Within recruitment methods, particular emphasis is placed on a competency-based approach and pre-employment assessments. Abd El Motaleb A. M. A. [3] recommends implementing competency models that evaluate both hard and soft skills through situational interviews and case-based tests, thereby precisely calibrating a specialist's profile to an organization's specific risk exposures. Ravichandran S. et al. [4] examine pre-employment testing practices in the U.S. and Australian hotel industries, demonstrating that combining cognitive tests with personality assessments yields the most accurate long-term reliability forecasts. At the same time, Sachan V. S. et al. [5] observe that AI can automate the preliminary sorting of candidates according to alignment with corporate values and threat profiles, though algorithmic bias and ethical considerations require further algorithm refinement.

Technological approaches to staff training are undergoing substantial transformation through the adoption of virtual and augmented reality, gamification, adaptive systems, and digital twins. Salama R. et al. [7] show that incorporating game elements into cybersecurity awareness programs for healthcare workers reduces errors when handling sensitive data by 30 percent after the first training cycle. PwC's research underscores that virtual reality and the metaverse can create immersive attack-response scenarios, significantly enhancing engagement and content retention [10]. However, Valluripally S. et al. [6] caution that such environments may introduce vulnerabilities—virtual labs can be targeted to undermine privacy or corrupt training data—necessitating specialized security protocols and continuous monitoring. Gligorea I. et al. [8] note the effectiveness of AI-driven adaptive e-learning systems: machine-learning–based platforms analyze learner progress and dynamically adjust learning paths, reducing time to acquire key skills by 20–25 percent. Similarly, Luo Q. et al. [11] explore the use of digital twins to simulate risk scenarios, enabling response drills for emergencies in a controlled setting and thereby reducing incident rates.

Finally, the integrity and reliability of assessment procedures in recruitment and training have been addressed by Garg M., Goel A. [12], who systematically analyze threats to online testing and propose integrity strategies ranging from biometric verification to real-

time user behavior monitoring. Hu S., Hsu C., Zhou Z. [9] emphasize that Security Education, Training and Awareness programs should combine formal coursework with continuous communication campaigns to cultivate an organizational "security culture".

Thus, the literature reveals several contentious and underexplored issues. Competency models and AI solutions demonstrate high effectiveness, yet ethical concerns and the potential for algorithmic discrimination remain. Conversely, immersive learning technologies (VR, digital twins) enhance engagement but their own vulnerabilities are not yet fully examined. Moreover, despite extensive discussion of assessment methods, research remains limited on long-term monitoring of trained specialists' performance and on the influence of corporate culture on security skill retention.

Results and Discussion

Based on the analysis and in order to address gaps identified in the literature, an Integrated Competency Model (ICM) has been developed for the selection and training of security service personnel. The central element of this model is seamless continuity between candidate assessment stages and the subsequent program of continuous professional development. The model follows a synergistic principle: the outcomes of each stage constitute the methodological and substantive basis for designing the content and methods of the following stages.

Stage 1: Multi-level Competency-Based Selection. The procedure begins with a rejection of a reductionist approach and the introduction of a hierarchical analytical system aimed at producing a complete psychophysiological and professional profile of the applicant. The proposed scheme comprises three interrelated evaluation levels, each of which performs a specific function in the selection process.

Level 1: Primary Formal Verification. This stage checks compliance with basic formal criteria: possession of relevant education, confirmed work experience, and absence of criminal records. Experts simultaneously review biographical information and submitted references. The main objective is to exclude individuals who clearly fail to meet the minimum requirements [5, 6].

Level 2: Comprehensive Psychodiagnostic Assessment. The core of the selection process is multifaceted testing designed to identify and assess key competencies grouped into three clusters (see Table 1). Validated instruments are employed: the Minnesota Multiphasic Personality Inventory (MMPI) for analysis of personality structure and detection of latent accentuations, the Holmes–Rahe Stress Scale for resilience measurement, and specialized tests aimed at determining the candidate's conscientiousness and loyalty.

Level 3: Situational Role Simulation. Candidates who successfully complete psychodiagnostics proceed to practical case resolution and Situational Judgment Tests (SJTs). Virtual-reality technology provides the greatest informational value: the applicant is immersed in an environment that reproduces the company's platform and is required to handle several non-standard scenarios—an attempted unauthorized entry, discovery of a suspicious object, and aggressive visitor behavior. Evaluation addresses not only the correctness of the actions taken but also reaction speed, the ability to remain composed, and decision-making under constraints of time and information [8, 10].

Table 1. Key competencies of security-service personnel and evaluation methods (compiled by the author based on analysis [3, 4, 7, 9])

Competency Cluster	Competency	Description	Evaluation Method
Cognitive-Analytical	Critical thinking	Ability to analyze information from multiple sources, identify inconsistencies, and forecast developments.	Analytical case studies; logical-reasoning tests
	Attention to detail and observation	Ability to notice small details and deviations from normal behavior or environment.	Concentration tests (e.g., Schulte tables); video-record analysis
Personal-Volitional	Stress resilience	Ability to maintain performance and make appropriate decisions under high psychological pressure.	Psychophysiological testing (EEG, GSR); Holmes–Rahe Stress Scale
	Responsibility and integrity	High level of self-control, adherence to rules and standards, honesty.	Polygraph (where legally permitted); integrity tests
	Decisiveness	Willingness to take responsibility for decisions in critical situations.	Situational-judgment tests; VR simulations
Communicative-Behavioral	Conflict management	Skills in negotiation, de-escalation of aggression, and persuasion.	Role-playing exercises; practical case scenarios
	Teamwork	Ability to interact effectively with colleagues to achieve common objectives.	Group exercises; observation during simulations

The outcome of the first stage is not a simple "accept or reject" decision but the creation of a detailed competency profile for each successful candidate, in which key strengths and priority development areas are systematically documented.

Stage 2: Adaptive learning architecture. The competency profile generated in the previous stage serves as the foundation for designing an individualized learning pathway. The proposed architecture relies on implementing employee digital twins and using adaptive learning platforms capable of dynamically adjusting both content and delivery format to the specific needs and learning pace of each professional.

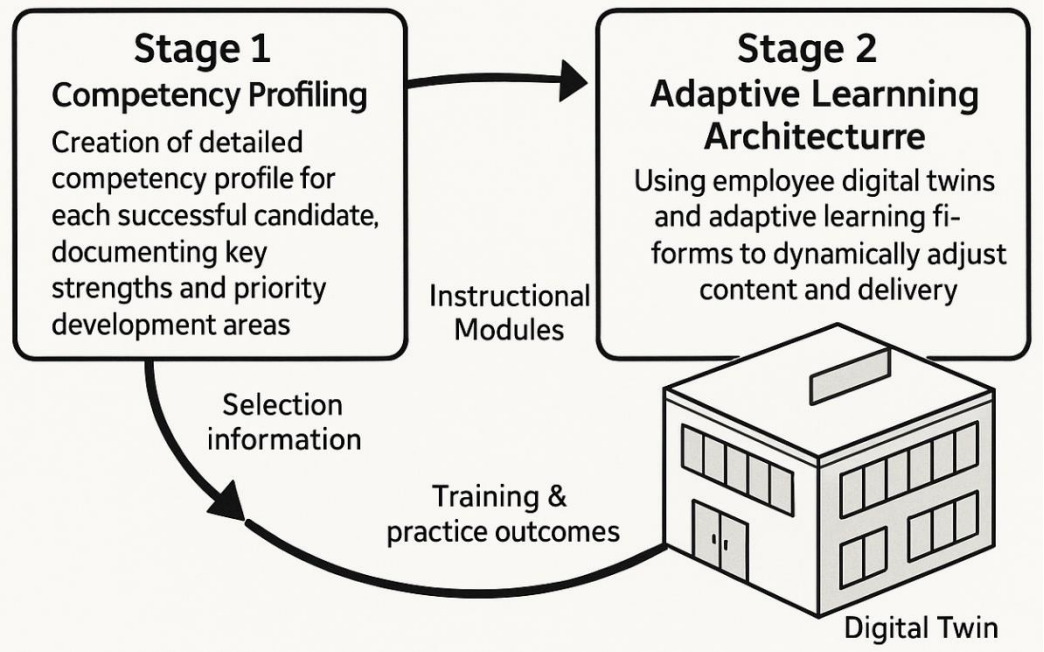

Fig. 1. Integrated competency model (ICM) for the selection and training of security personnel (compiled by the author based on the analysis of [4, 11, 12]).

According to the scheme shown in Figure 1, the model operates as a continuously functioning cycle: information obtained during candidate selection determines the structure and content of the instructional modules, whereas the outcomes of training and practical activities supply the evidence base for refining the competency profile and adapting the programme itself.

The instructional process relies on the deployment of a digital twin of the protected facility—an exact virtual replica of the company's building, office, or production site. Within this highly detailed environment, regular training exercises are conducted through virtual-reality technologies, closely replicating real work scenarios.

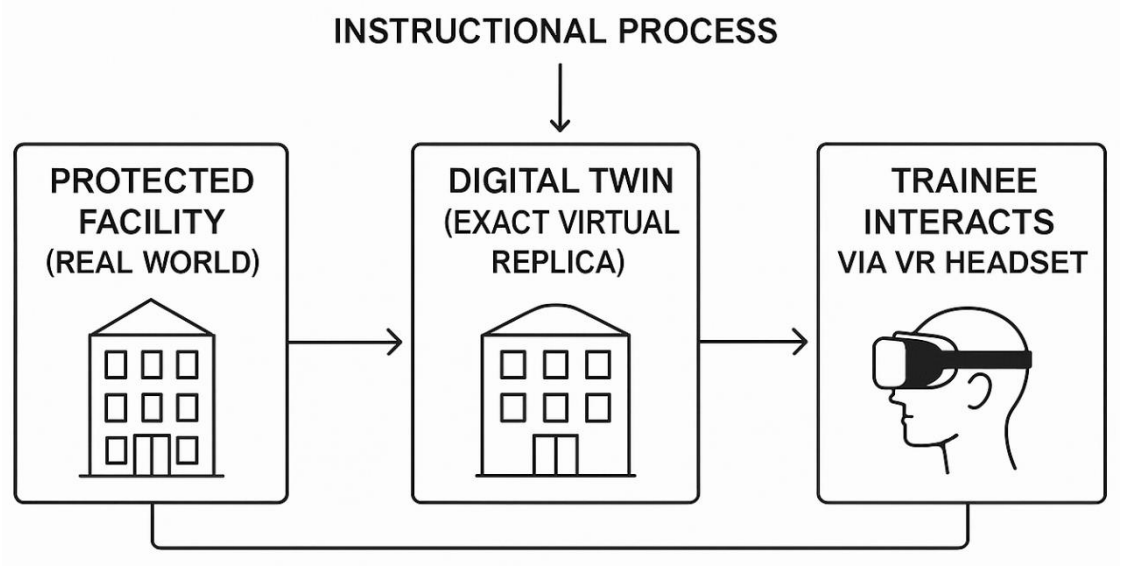

Fig. 2. Architecture of adaptive learning based on a digital twin (compiled by the author based on the analysis of [6, 8]).

The effectiveness of the Integrated Competency Model (ICM) is assessed through an expanded set of criteria: alongside classical KPIs—such as the number of incidents averted—additional metrics are introduced that capture the depth and quality of staff professional development.

The proposed integrated competency model fundamentally restructures the linear logic of "selection – training – assignment," transforming human-capital development in the security domain into a continuous, self-regulating system. Through the synergy of psychodiagnostic methodologies and a flexible educational architecture, three key effects are achieved. First, predictive accuracy in candidate selection increases: the organization receives not an abstract résumé but a clearly measurable profile of applicant potential. Second, training resources are allocated purposefully; instead of one costly universal course for all professionals, investment is directed toward strengthening only those competencies required by each specific employee. Third, a proactive security paradigm emerges in which graduates of adaptive VR simulations acquire not merely action algorithms but flexible behavioral patterns enabling effective responses to previously unseen, atypical situations [10, 11].

Despite its obvious strategic advantages—mitigating the human factor, reinforcing business resilience, and safeguarding reputation—the implementation of such a system entails significant challenges. Major barriers include substantial expenditures for developing reliable digital twins and VR scenarios, the need to recruit highly qualified psychometricians and virtual-reality specialists, and potential resistance to change among personnel and conservative management. Nevertheless, the long-term benefits overwhelmingly outweigh the initial investments.

Conclusion

The study systematized contemporary theoretical and methodological approaches to selecting and training security personnel in large enterprises and revealed a fundamental gap between assessment procedures and training programs. To eliminate this fragmentation, a substantiated Integrated Competency Model (ICM) is proposed. The model forms a closed, cyclical process that integrates in-depth psychodiagnostics during the selection phase with an adaptive training architecture that employs immersive technologies.

The main findings are as follows:

Maximum effectiveness in security-staff selection is attainable only through comprehensive, multi-level analysis. The emphasis must shift from formally stated requirements to the evaluation of cognitive-analytical, personality-volitional, and communicative-behavioural indicators by means of validated psychodiagnostic methods and situational exercises.

Innovative training techniques—particularly the application of digital twins and virtual simulations—make it possible to move from generic courses to personalized, adaptive programs. This approach facilitates deeper acquisition of professional skills and fosters resilient behavioural strategies in extreme conditions.

The key element of the ICM is the employee's "competency passport," created at the selection stage and forming the basis for an individual learning trajectory. Targeted work on identified development areas and reinforcement of existing strengths optimize resources and increase training efficiency.

The proposed model offers large corporations a concrete tool for systematically strengthening the human capital of their security departments, directly mitigating operational, financial, and reputational risks amid rapidly evolving external threats.

References

1. Cost of a Data Breach Report 2023. [Electronic resource]. - Access mode: https://www.ibm.com/reports/data-breach (date of access: 12.05.2025).
2. Gartner Identifies the Top Cybersecurity Trends for 2024. [Electronic resource]. - Access mode: https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024 (date of access: 15.05.2025).
3. Abd El Motaleb A. M. A. Competency-based human resources management (case study) //Middle East Journal for Scientific Publishing. – 2021. – Vol. 3 (3). – pp. 42-72.
4. Ravichandran S. et al. Pre-employment testing practices in the hospitality industry in the US and Australia //Journal of Human Resources in Hospitality & Tourism. – 2022. – Vol. 21 (4). – pp.

524-547. https://doi.org/10.1080/15332845.2022.2106614.

5. Sachan V. S. et al. The Role Of Artificial Intelligence In HRM: Opportunities, Challenges, And Ethical Considerations //Educational Administration: Theory and Practice. – 2024. – Vol. 30 (4). – pp. 7427-7435.
6. Valluripally S. et al. Detection of security and privacy attacks disrupting user immersive experience in virtual reality learning environments //IEEE Transactions on Services Computing. – 2022. – Vol. 16 (4). – pp. 2559-2574. https://doi.org/10.1109/TSC.2022.3216539.
7. Salama R. et al. Using Gamification to Increase Healthcare Professionals' Cybersecurity Awareness //International Conference on Smart Applications and Sustainability in the Artificial Intelligence of Things. – Cham : Springer Nature Switzerland, 2024. – pp. 915-922.
8. Gligorea I. et al. Adaptive learning using artificial intelligence in e-learning: A literature review //Education Sciences. – 2023. – Vol. 13 (12). https://doi.org/10.3390/educsci13121216.
9. Hu S., Hsu C., Zhou Z. Security education, training, and awareness programs: Literature review //Journal of Computer Information Systems. – 2022. – Vol. 62 (4). – pp. 752-764. https://doi.org/10.1080/08874417.2021.1913671.
10. What does virtual reality and the metaverse mean for training? [Electronic resource]. – Access mode: https://www.pwc.com/us/en/tech-effect/emerging-tech/virtual-reality-study.html (date of access: 18.05.2025).
11. Luo Q. et al. Applications of digital twin technology in construction safety risk management: a literature review //Engineering, construction and architectural management. – 2024. - pp. 3587-3607. https://doi.org/10.1108/ECAM-11-2023-1095.
12. Garg M., Goel A. A systematic literature review on online assessment security: Current challenges and integrity strategies //Computers & Security. – 2022. – Vol. 113. https://doi.org/10.1016/j.cose.2021.102544.