Postprint of Applying Dynamic Security Models to Construct Information Security Management Systems

Authors: Mei Chunlin

Date: 2023-10-08T00:00:00+00:00

Abstract

While implementing information technology construction, related work on information security is also being steadily advanced. In recent years, both domestic and international researchers have been investigating how to leverage security frameworks and analytical design models to maximize the effectiveness of information security technologies and management methodologies. Therefore, this paper analyzes and interprets dynamic security models from the perspectives of information security management and the achievement of specific security objectives, systematically reviews and analyzes the construction of information security management systems, proposes recommendations for improving and refining such systems, and seeks to develop a novel approach for establishing an information system security service architecture.

Full Text

Applying Dynamic Security Models to Construct Information Security Management Systems

Abstract: As organizations advance their informatization initiatives, related information security work is progressing steadily. In recent years, both domestic and international research has focused on leveraging security frameworks and analysis/design models to maximize the effectiveness of information security technologies and management methods. This paper analyzes and interprets dynamic security models from the perspectives of information security management and specific security objective achievement, systematically examines the construction of information security management systems, and proposes recommendations for improvement, thereby offering new approaches for establishing information system security service architectures.

Keywords: Information security management system; Management framework; Dynamic security model; Systematic management approach

1.1 Overemphasis on Technology, Neglect of Management

Many organizations manage information system security primarily through business and technical service outsourcing models. However, outsourced service providers exhibit uneven security capabilities and often fail to implement effective security measures.

1.5 Insufficient Attention to Security in System Construction

System construction units frequently invest heavily in functionality while neglecting security, creating substantial hidden risks for subsequent operations and maintenance. Many organizations operate under the misconception that deploying certain technical protection measures alone can guarantee system security, yet they lack enforcement of supporting management rules and regulations. This leads to frequent last-minute, "exam-oriented" approaches when conducting security inspections, gap analyses, and system security level testing. In the construction of technical system operations, management, and regulatory frameworks, information security is often conspicuously "absent," and when conflicts arise between business operations and information security, security typically yields to business priorities.

1.2 Lack of "Improvement" and "Service" Thinking

Many information system managers still maintain a reactive mindset, viewing security protection as adequate as long as "no problems occur." However, as the information security threat landscape becomes increasingly urgent, security work cannot afford to wait for incidents to occur before receiving attention; it should instead become a driver for information system development and innovation. Information security should be a dynamic, continuous improvement process, approached with a "service-promoting" mindset that emphasizes ongoing enhancement.

2. Establishing an Information Security System Using Dynamic Security Models

To address existing problems in information security management and construct a security system that complies with relevant regulations while adapting to business development, a fundamental mindset shift is required—transforming information security from a "strict defense" posture to "proactive" dynamic thinking. Toward this end, security evaluation and analysis models can serve as references, with management analysis methods and tools applied to construct

an evaluation framework that objectively describes problems, solutions, and improvement areas in information security work.

1.3 Information Security Systems Not Formed into a Cohesive Framework

In all information security work, people are the critical element. Many information security management units provide inadequate security knowledge promotion and training, resulting in poor security awareness among personnel. Furthermore, many organizations lack appropriate security policies, and their established management systems fail to form cohesive frameworks. The absence of process-oriented, standardized security management systems that can be strictly enforced in daily operations creates numerous challenges for information security efforts.

1.4 Inadequate Responsibility Management

Many organizations disperse security administrator responsibilities among frontline technical operations and maintenance personnel without establishing dedicated security administrator positions. When ordinary system administrators perform security tasks, they tend to focus primarily on equipment and system operation status while struggling to objectively assess system security from an information security perspective or accurately implement security regulations and management frameworks. Simultaneously, establishing corresponding risk evaluation mechanisms can enhance the proactivity of information security management.

2.1 P2DR2 Dynamic Security Model-Based Information Security Management Framework

In information security management, personnel organization, security technology, and operations constitute three primary support systems. The core concept of the P2DR2 dynamic security model involves constructing and managing these three systems through integrated technical and management approaches to build a complete information security management framework. During framework construction, overall security policies must first be established, with various measures employed to understand and assess information system status, adopt appropriate response and recovery measures, reduce system security risks, and mitigate risks arising from security incidents.

2.1.1 Protection Phase The protection phase ensures network-level structural security, access control, boundary integrity checking, malware and intrusion prevention, and network device protection. At the host level, it includes intrusion prevention, malware prevention, identity authentication, system access control, system resource control, data protection, security feature labeling, and network trusted path protection. At the application level, it encompasses iden-

tity authentication, access control, communication integrity, software fault tolerance, communication confidentiality, resource control, residual information protection, non-repudiation, security labeling, and trusted paths. At the data level, it includes data integrity and data confidentiality. Various technical tools and methods can be employed, including multi-function firewalls, network switching and routing devices, intrusion detection systems, data gateways, patch reinforcement systems, anti-virus systems, operating system reinforcement devices, and database reinforcement devices, with secure configurations serving as necessary supplements.

2.1.2 Monitoring Phase To ensure information systems are protected from intrusion and damage by security incidents, measures such as intrusion detection, vulnerability scanning, security auditing, anti-virus gateways, and security management center monitoring can be adopted.

2.1.3 Response Phase Security response encompasses network and system security management, coordination and cooperation mechanisms, specific handling of security incidents, and revision and drills of emergency response plans. These can be implemented through security auditing systems, network operations and maintenance management systems, combined with professional technical support services and emergency response services.

2.1.4 Recovery Phase The recovery phase requires redundant designs for system and data backup and recovery to ensure information systems can be promptly restored to operation.

2.2 Using Systematic Management Methods for Security Assessment

After constructing an appropriate information security management framework using the P2DR2 model, systematic management methods (ISMS) can be applied for security situation assessment. Assessment work is based on risk information and divides information security into phases including establishment, implementation, operation, monitoring, review, maintenance, and improvement. Key principles include: (1) covering all aspects of information security work and establishing corresponding regulations and management frameworks; (2) scientifically analyzing various elements within the information security management framework and comprehensively considering potential issues in each phase; (3) archiving and managing various log files and process information; and (4) ensuring effective feedback of all information security-related information.

2.3 Using PDCA Method to Establish Information Security Management System

Following the completion of information security management framework establishment and security situation assessment, the information security man-

agement system can be constructed using the "Plan-Do-Check-Act" (PDCA) model.

2.3.1 Plan Phase *Determine ISMS scope and policy:* The information security management system should encompass all stages of information security work, clearly define its scope, establish security policies relevant to the information security environment, and manage, protect, and allocate information assets.

Define risk assessment methods: During risk assessment, appropriate methods must be selected and grading criteria determined. Risk assessment documents should be developed to explain the employed methods, techniques, and tools, as well as the business context of their application. Additionally, various assets and vulnerabilities within the scope should be accurately estimated to assess potential impacts when security incidents occur.

Identify, assess, and control risks: This phase's primary task involves classifying impact levels when various assets experience losses in vulnerability, confidentiality, integrity, and availability, thereby correctly assessing losses caused by risks. Risk control methods must also be selected to achieve risk control objectives, prevent, stop, and limit risks, and implement recovery controls.

Unified management planning: During ISMS establishment, unified planning and clear task objectives are required, along with corresponding management authorization to facilitate normal system construction progress.

2.3.2 Do Phase *Establish the ISMS:* This process involves the specific implementation of management processes, regulations, and planning. Through concrete analysis of risk assessment, risk identification, and risk control, appropriate resources (personnel, time, and funds) are allocated to develop targeted response measures for various risks.

Promote and apply the management system: During ISMS promotion and application, all regulations should be implemented, relevant personnel should receive security training, and each position's role and responsibilities should be clearly understood. By continuously strengthening security awareness, all parties can complete tasks according to requirements.

2.3.3 Check Phase The Check phase is a critical stage in the PDCA cycle, analyzing operational effectiveness and seeking improvement opportunities. Its purpose is to promptly correct unreasonable, insufficient, or difficult-to-implement measures during execution. Specific content includes: checking for errors in implementation; whether information security management tasks achieve expected results; and accepting third-party security inspections. This phase also involves evaluating ISMS effectiveness, collecting relevant suggestions and feedback, conducting regular effectiveness reviews, determining risk impact scope and degree, and implementing risk control.

2.3.4 Act Phase In the Act phase, conclusions must be drawn about proposed implementation plans, assessing the usability and sustainability of the information security management system, and planning for its promotion and promulgation.

2.4 Other Issues to Consider When Establishing Information Security Management System

2.4.1 Supplementing the Improvement Phase in PDCA Reviewing the entire process of establishing an information security management system through dynamic security models reveals that while the P (Plan), D (Do), and C (Check) phases of PDCA are well-executed, the A (Act) phase may lack specific means and measures, hindering ISMS correction and improvement. Therefore, in the improvement phase of establishing a new security management system, it is necessary to fully communicate with operational departments, identify problems, propose solutions, and provide a foundation for system improvement. Additionally, through pilot promotion, survey feedback, and data statistics, information about actual operational effectiveness should be obtained to evaluate practical performance. Content that proves inefficient, inconsistent with business operations, or difficult to implement should be revised or removed.

2.4.2 Establishing Diversified Security Linkage Mechanisms During ISMS construction and promotion, multi-level, multi-system collaborative management mechanisms exist. Therefore, based on the information security management system, diversified security linkage mechanisms should be established, including monitoring and notification mechanisms, command and coordination mechanisms, information feedback mechanisms, and emergency response mechanisms. For various emergency events, detailed and feasible security incident handling procedures should be established, following principles of unified command, unified coordination, unified interfaces, unified reporting, and unified feedback. Regular security emergency drills should also be conducted.

2.4.3 Emphasizing Dedicated Security Personnel Training During ISMS construction, the training mechanism for dedicated security personnel should be strengthened. Information security talent cultivation must be enhanced. In addition to frontline technical personnel mastering various security attack and defense technologies and possessing capabilities for attack detection and prevention and system protection and recovery, security management personnel also need capabilities in system security planning, risk analysis, emergency response, and security auditing. They should formulate information security plans at the organizational level and organize and direct implementation.

2.4.4 Establishing ISMS Evaluation Methods How to measure the performance of an established information security management system and evaluate its operational effectiveness in practical implementations are important

considerations during system construction and promotion. (1) Meeting organizational information security management needs: The purpose of establishing an ISMS is to streamline internal security management mechanisms, effectively respond to emergencies, improve information security management levels, and enhance control capabilities over various information security risks. Therefore, actual work requirements can serve as a checklist for evaluation and correction during work to meet practical management needs. (2) Using comprehensive evaluation metrics: Since ISMS establishment, promotion, and use do not generate direct benefits, comprehensive evaluation methods based on organizational characteristics can objectively assess system effectiveness. For example, collecting opinions from various departments, management personnel, technical staff, and users; comparing quarterly or annual information security management system operation statistics; and comparing security work efficiency and personnel workload before and after system implementation. (3) Establishing personnel assessment and evaluation systems: Personnel security literacy is closely related to information security management capabilities, core protection capabilities, and risk prevention capabilities. Therefore, regular personnel quality inspections and assessments can be organized to comprehensively evaluate security technology application, management process control, and coordination work handling. Problems can be corrected based on assessment results to enhance organizational operational efficiency, improve professional skills, and promote healthy organizational development.

References

[1] Xie Zongxiao. Information Security Management System Implementation Guide [M]. Beijing: China Standards Press. 2012.
[2] Zhang Zehong, Zhao Dongmei. Information Security Management and Risk Assessment [M]. Beijing: Electronic Industry Press. 2010.
[3] Wang Zhenxue, Zhou Anmin, Fang Yong, et al. Information System Security Risk Estimation and Control Theory [M]. Beijing: Science Press. 2011.
[4] Liu Xiaomin, Xu Lei. Analysis of the Definition, Function, and Construction Methods of Information Security Management Systems [J]. Information & Communications. 2013(1).

(Author's affiliation: Xinhua News Agency Technical Bureau)

Note: Figure translations are in progress. See original paper for figures.