Technical Framework Research on Critical Information Infrastructure Cybersecurity Classified Protection

Ren Weihong[a], Yuan Jing, Jiang Lei, Zhao Tai

The Third Research Institute Of Ministry Of Public Security; Beijing, China

[a]email:renweih@cspec.org.cn

Keywords： Critical Infrastructure; Critical Information Infrastructure; Classified Protection; Management and control capability; Security control

Abstract. The technical framework of critical information infrastructure cybersecurity classified protection in this paper is established from the three levels of decision-making, managers and executives which ensures the information security technical framework of an organization is consistent with its strategic business objectives. At the same time, on the base of testing and evaluation for security classified protection, evaluation of management and control capability is conducive to evaluate the information security situation of an organization. The assessment of management and control capability combines the strategic business objectives and classified protection which is beneficial to promote organization's innovation and initiative.

Introduction

At present, critical information infrastructure protection has become a new focus of international cybersecurity legislation and technology research. China's cybersecurity classified protection system practice provides a successful experience for critical infrastructure cybersecurity protection. At the same time, the development of new technologies and new applications has stimulated the model innovation of cybersecurity classified protection of critical infrastructures. The research results of this paper not only perfect the cybersecurity classified protection technology system has a direct role in promoting, but also the selection of cybersecurity controls and the evaluation method of cybersecurity protection situation can be used in critical information infrastructure sector evaluates its situation of cybersecurity protection.

Background

Since Ministry of Public Security cooperating with other three Ministries published file “Classified Protection of Information Security Government Rule” (MPS [2007]43) was released in 2007, system's class determination, registration, construction, rectification, classified security testing and evaluation according to national standards "GB/T 22240-2008Classification guide for classified protection of information system”, "GB/T 22239-2008 Baseline for classified protection of information system”[1], "GB/T 25070-2010 Technical requirements of security design for information system classified protection”[2] has played an important role in safeguarding China's important information system.

With the improvement of protection capability in various fields and the emergence of new technologies and applications, the existing practices that system construction based on GB/T 22239-2008, standard compliance testing and evaluation as the main evaluation method, the design concept of the original system according to GB/T 25070, have been unable to fully meet the growing security needs of critical information infrastructure in various fields of cybersecurity protection. The classified protection in sectors has also been carried out for many years. Over years of the construction and rectification of systems, many the-third-class systems has reached a steady state in compliance to the national standard. But the security needs and faced threats of information system did not stop. Therefore, it is necessary to study and design a new technical system with greater applicability and openness to perfect the classified protection system.

Framework Structure Design

According to the requirement of cybersecurity classified protection policy and standards, a critical information infrastructures can be further divided into different classified objects according to the importance of the different business they carry, and determine the classified object's class. A critical information infrastructure may include one or several classified objects, and the classified objects‘ classes may be different. The relationship between a critical information infrastructure and classified objects is shown in Fig. 1.

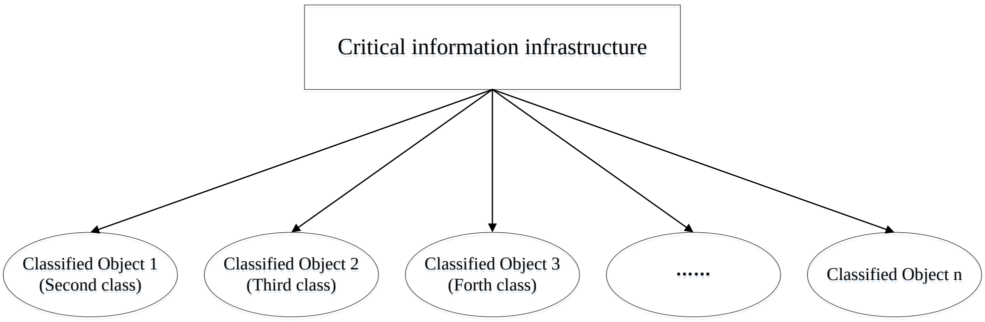

Fig. 1.Relationship between a critical information infrastructure and classified objects

Critical information infrastructure protection requires the participation of decision-makers, managers and the executives. The decision-makers are responsible for determining the cybersecurity protection strategy of organization from the perspective of protecting the infrastructure security, which determines the overall security goal of the organization's infrastructure cybersecurity. The security goal guides the managers to determine the organization's information security policy and formulate information security architecture. The security policy as determined by the managers guides the executives to determine the security protection capabilities to be achieved by each classified object, along with the security functions and safety procedures to be taken. The executives are responsible for the operation management and maintenance of the classified objects.

Fig.2 shows the cybersecurity classified protection technology framework. The framework describes the relationship of the three-tier architecture of critical infrastructure, security control set and capabilities evaluation. The three-tier architecture describes the information security concerns of the decision-makers, managers and executives, and the relationship of them. Security control set is built the complete set of security control types based on IPDRR model [4]. It provides a technical line for the establishment of critical infrastructure security mechanism, and guides the organization to select appropriate security controls. To examine the actual achievement of the cybersecurity assurance strategy for critical infrastructure, capability evaluation from the two aspects of classified object and critical infrastructure is introduced. The capability evaluation includes the system's security capability evaluation and the cybersecurity control capability assessment of the critical infrastructure.

Security Control Set

The security control set provides a set of security controls that can be taken to achieve the business mission for the critical information infrastructure. The sources of security controls are the main standards, guidelines, and practices for information security. The security control set itself is not the basis for security assessment, examination and evaluation, but it provides a choice of functions and activities for managing information cyber security risks and realizing information security. The security control set consists of six elements: Functions, security control Categories, security control Subcategories, Description, corresponding Level and System or Organization.

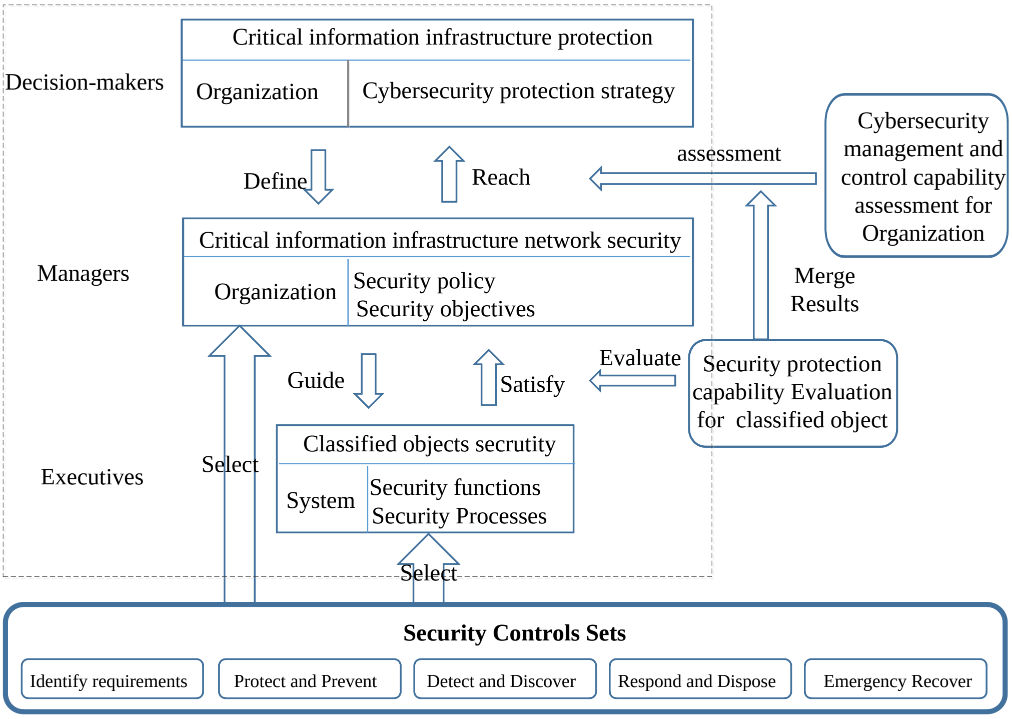

Fig.2. cybersecurity classified protection technical framework

Functions organize basic cyber security activities at their highest level in organization. With reference to the common security model and best practices for security implementation, Functions include five areas with timing characteristics: Identify requirements, Protect and Prevent, Detect and Discover, Respond and Dispose, Emergency Recover. From the perspective of organization managers, Functions follow the general approach of security incident management, and reflect the risk management decision-making process, which help display the effectiveness of cybersecurity. All security control Categories and Subcategories belong to different Functions, indicating that these security controls on the role of security protection and risk control are different. Critical infrastructure can have their own choice to strengthen the security control capability of certain functions based on ensuring the basic security protection capabilities, according to their own security strategy and the requirement to confront the threats.

Security control Categories are the subdivisions of a Function into groups of cyber security controls closely tied to effects and particular activities.

Security control Subcategories further divide a Category into specific outcomes of technical and/or management activities. Subcategories are intended to cover all known activities to achieve the effects of the Category from different aspects.

Description is a summary description of the Subcategories control measures.

Corresponding Level: Subcategories security controls have different implementations, and the security function strength of different implementations will also be different. Corresponding Level gives the correspondence between security control Subcategories and "GB/T 22239 Baseline for classified protection of information system".

The security control set centralizes security controls from GB / T 22239, ISO / IEC 27001 and NIST SP800-53 etc [5][3]. The five Functions extended on the base of PDR model, are classified as the highest level of security controls, which reflects the risk management decision-making process and helps to demonstrate the effects of cybersecurity.

With the emergence of new technologies and new threats, the control sub-category of the security control set will also be expanded, but the control category can remain stable basically unchanged.

Evaluation According to the Framework

The evaluation of the critical infrastructure cybersecurity includes the evaluation of the security protection capability of the classified object (including information system, control system and communications network, referred to as the "Object evaluation") and the assessment of the capability of the organization management and control (referred to as the "Organization assessment"). Organization assessment is based on Object evaluation that determines the scope and focus for it. Organization assessment assesses the effectiveness and implementation ability of the organization cybersecurity work synthesizing the outcomes of Object evaluation.

Object Evaluation. Object evaluation is carried out for the classified object, which includes classified security testing and evaluation and customization classified security testing and evaluation. The target of classified security testing and evaluation is classified object.

The evaluation metrics are corresponding baseline for classified objects. Classified security testing and evaluation can evaluate the compliance between the object security protection status and cybersecurity baseline.

Customization classified security testing and evaluation focuses on whether the security functions, activities, and processes implemented by the classified objects fulfill the security policies and objectives defined by the organization's managers. The evaluation metrics are the target metrics. The evaluation can evaluate the compliance between the object security protection status and target metrics defined by organization.

Organization Assessment. Organization assessment is carried out for the organization, which assesses the security control execution of organization. The assessment is implemented by assessing the organization's willingness, ability and degree of completing information security work.

Based on the evaluation outcomes of multiple classified objects, the assessment verifies whether the security protection capability and effect of the classified objects are satisfied of the security policies and targets defined by the organization's managers from managers activities controllability and security mechanism effectiveness. At the same time, based on the outcomes of Objects evaluation and organization management activities, the assessment verifies and analyzes whether organization cybersecurity work has reached the organization cybersecurity strategy.

The cybersecurity management and control capability of the evaluated object includes three tiers: disorder, order and evolution. The tiers describe an increasing degree of implementation of cybersecurity work, and tightness of entire organization mission with cybersecurity work. Organization can choose the appropriate tier to reduce cybersecurity risks for critical infrastructure. Organization also should accord to the specific circumstancesto ensure that the chosen tier is actually effective and economically viable.

The assessment metrics of cybersecurity control execution of organization includes six aspects:

- Willingness: The degree of decision-makers' cybersecurity awareness;
- Policy enforcement: The degree of implementation of the established safety management system;
- Technology implementation: The implementation effectiveness of technical measures such

as identification, protection, detection, response and recovery;

- Human resources: Managers and control capability of managers to cybersecurity-related human resources;
- Information sharing: The ability of the organization to acquire and utilize cybersecurity information;
- Measurement: the ability of the organization to evaluate the work of cybersecurity;

The execution assessment metrics system not only enables an organization to clarify the objectives and the status of its own information security work and provides the basis for continuous improvement activities, but also it enables an organization to conduct horizontal comparisons with other organizations in the same sector and expands space to improve the capability of the sector's information security.

Conclusion

Based on the current practice of putting forward the baseline metrics for a classified object, the method is proposed that determines and dynamically adjusts target metrics of a classified object according to its security requirements and taken controls. The target metrics are used to meet classified protection requirements and an organization's own security policies and objectives.

Based on the IPDRR model, this paper builds a set of security controls which include all network security control categories. The Framework guides organizations to construct classified protection security system of the critical infrastructures based on classified objects classified protection.

The conformity evaluation according to GB/T 22239 is been extended to include customized evaluation according to classified objects target metrics and cyber security control capability assessment of the critical infrastructure.

Technical Framework research on critical information infrastructure cybersecurity classified protection can guide an organization to implement classified protection system and construct a safety assurance system in line with their own risk control objectives. Framework can be more accurate evaluation of a critical infrastructure cybersecurity effectiveness. It will make up the vacancy that the information security classified protection system only protect information systems as the goal for a long time, extending from the information systems protection to dimensional security protection of entire enterprise, group or sector. It is conductive to ensuring the sustained and healthy development of China's classified protection system.

References:

[1]GB/T 22239-2008, Information Security Technology-Baseline for Cybersecurity Classified Protection [S].Beijing: China Standard Press, 2008.

[2]GB/T 25070-2010 Information security technology-Technical requirements of security design for information system classified protection [S]. Beijing: China Standard Press, 2010.

[3]NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations V4.0.

[4]Framework for Improving Critical Infrastructure Cybersecurity. [EB/OL]. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[5]GB/T 22080 Information Technology-Security Technology-Information Security Management Systems[S]. Beijing: China Standard Press,2008.