Risk Management Theory Application in national information security risk control—Analysis of the relationship between classified protection and risk management

Maning Bi, Yuan jing

MPS Information Classified Security Protection Evaluation Center，The Third Research Institute Of Ministry Of Public Security，Beijing, 100142, China

Keywords: information security, classified protection, risk control and management.

Abstract. The risk management theory has been applied in information technology area for many years. And it has been regarded as an effective information security solution and approach. With the full expansion of information classified security protection implementation, persons are puzzled by the relationship between classified protection and risk management. This paper analyzes that the information security classified protection is the Chinese-specific risk management and control system for information security.

Introduction

The information revolution, started mid last century, fundamentally changed the ways people live and work, just like every other industrial revolution during human history. The development of information technology, especially the communication technologies based on TCP/IP, such as world wide web, platform sharing, resource sharing, bring about enormous changes to the way people live and work. Nowadays, governmental affairs, social stability and people's daily lives all depend on computer information systems. As we enjoy the increased comfort and convenience brought by the information revolution, security threats are emerging.

Information security classified protection is national fundamental policy to raise information security protection class and capability, to protect national security, social stability and public interest, to ensure and enhance healthy development of information technology during the process of economic development and technological advancement. In order to promote implementation of the information classified security protection, the Ministry of Public Safety drafted supportive policy and standards for information classified security protection together with other relevant ministries based on "People's Republic of China Computer Information System Security Protection Ordinance" (Policy #147). The document, "Supervising measures for information classified security protection" (GongTongZi[2007]#43) clarifies the important tasks, such as class determination , implementation and rectification, class assessment, monitoring and inspection.

As the information classified security protection effort is underway, more and more information system operators and users, security providers, and product manufacturers across the country have joined in this effort. The information classified security protection methodology has drawn attentions never seen before. With the full expansion of information classified security protection implementation, more questions arise regarding to the relationship between the classified protection scheme and risk management methods. This paper points out that the information classified security protection is the Chinese-specific risk management and control system for information security.

Theoretical development of information security protection risk management

Any organization, whether it is a government agency, or a corporation, its purpose of existence is to bring value to the vested party in such an entity. The challenge of the organization is to accept the uncertainty while pursue maximum value acquisition. Uncertainty represents risk, as well as opportunity. Management of uncertainty is equivalent to management of risk. The modern risk management theory and practice originated from the western nations, and it was created for the purpose of effectively formulating economical development and market competition strategies. Due

to its wide applicability, the risk management theory has been adopted in many fields by most countries, including social development, economical development, public safety and information security.

Risk management theory was first applied to IT security in 1960s. At the time, with the emergence of resource-sharing computer systems and early computer networks, the problem of computer security first presented itself. In 1990s, due to the rapid growth of the Internet, mobile communications, and international network connections, information security becomes a common challenge around the world. Meanwhile, risk management theory and practice has made dramatic progress as well.

The International Organization for Standardization (ISO) published ISO/IEC 13335: Guidelines for the Management of IT Security in 1996, and ISO/IEC 15408: Evaluation Criteria for IT Security, and ISO/IEC 177799 (27002): Code of practice for information security in 2000. The widely-accepted IT security risk management theory and practice was first introduced in ISO/IEC 13335.

IT Security Risk Management in Different Countries

Research progress in IT security risk management theory and practice in various countries is further boosted by the publication of international IT security risk management standards. Though the standard elements and the finer details of IT security risk management differ from county to country, the core concept is the same, which includes scope determination, risk evaluation, risk control and risk monitoring. With the convergence of IT security risk management theory and practice, the research focus in each country is increasing based on its practical situations to explore an effective methodology for IT security risk management.

United States have the most advanced information systems, and is leading the way in IT security theory and practice. NIST published SP800-37 “Guidelines for Applying the Risk Management Framework to Federal Information Systems” in 2004, which explored how the risk management methods could be applied to federal information system security practice. After putting into practice for a few years, a revised version was published later.

Fig.1 shows the idea and approach adopted by US Federal information systems. The entire IT Security management process is divided into following steps: Categorizing information systems, Selecting Security Controls, Implementing Security Controls, Assessing Security Controls, Authorizing Information Systems and Monitoring Security State. Given all these steps, the federal government relies on NIST to perfect the policy and standard systems. The relevant stands include FIPS 199, SP 800-60, FIPS 200,SP 800-53, SP 800-70,SP 800-53A,etc.

Categorizing Information Systems is to determine the security categorization of information or an information system based on the potential impact if the system’s security is comprised. The main standards for this step are “Standards for Security Categorization of Federal Information and Information Systems” (FIPS 199), and “Guide for Mapping Types of Information and Information Systems to Security Categories” (SP 800-60).

Selecting Security Controls is to select the lowest (baseline) security controls based on the categorization of the information system, and apply relevant modifications. The main standards for this step are “Recommended Security Controls for Federal Information Systems” (SP 800-53), and “Minimum Security Requirements for Federal Information and Information Systems” (FIPS 200).

Implementing Security Controls is to implement security and management methods in an information system, including deploying security control products and inputting security configurations. The main standard is “Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developer” (SP 800-70).

Assessing Security Controls is to measure the effectiveness of the security controls, i.e. if the security control is implemented correctly, and is used correctly, and the implementation meets the security requirement. The standard involved is “Guide for Assessing the Security Controls in Federal Information Systems and Organizations” (SP 800-53A).

Authorizing Information Systems is to confirm that the current security state of an information system poses only acceptable risk to the operating organization, asset or individuals, and authorize

the operation of the system. The standard involved is “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach” (SP 800-37).

Monitoring Security State is to continuously track and monitor the changes in the information system itself or its operating environment that may impact information security, and if necessary, re-evaluate the effectiveness of the security controls and recommend improvement. The standards involved are “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach” (SP 800-37) and “Guide for Assessing the Security Controls in Federal Information Systems and Organizations” (SP 800-53A).

The process in Fig.1 is the guideline for how to apply IT security risk management framework to the federal information systems. While simplifying the technology and process, based on the characteristics of the federal information system, the administration management steps are added, i.e. Authorizing Information Systems, which only allow operation of an IT system when its current security state poses acceptable security risk.

The US President Obama submitted “The 44th President’s Cyber Security Evaluation Report”, indicating that the threat from cyberspace has become one of the most severe threats to US economy and military. Cyberspace and the threat associated with it are real, and protecting the network infrastructure has become the most important part of national security. “Cyberspace is a critical asset for our country. We need to protect it with all of our power, to protect the country and its citizens, the economic development, and smooth delivery of critical services.”

Classified Protection is IT Security Risk Management with Chinese Characteristics

How do we learn from the existing IT security risk management framework, and apply it to the unique information system management circumstances in China, to open up a new path of classified security protection that is suitable for our IT information management situations? The classified IT security protection is an important step in constructing our country’s IT security system. It is also a basic policy for IT security. How do we fully utilize the IT security supervising agency’s functions during implementation of the policy? To achieve this goal, the Ministry of Public Safety and other relevant ministries started to draft the documents: “Opinions on the Implementation of Information System Classified Security Protection” (GongTongZi[2004]#66) and “Supervision Methods for Information Classified Security Protection” (GongTonZi[2007]#44), which clarified the steps in a classified security protection implementation, including Class Determination, Implementation and Rectification, Class Assessment, and Monitoring and Inspection.

The process as shown in Fig.2 is created for Information Classified Security Protection implementation based on risk management framework and the characteristics of our information systems. The corresponding standard documents include “Guide on Information system security classified protection class determination”, “Basic Requirements for Information System Security Classified Protection”, “Requirements for Assessment and Evaluation of Information System Security Classified Protection”, and “Guidelines and Requirements for Assessment and Evaluation Process of Information System Security Classified Protection”.

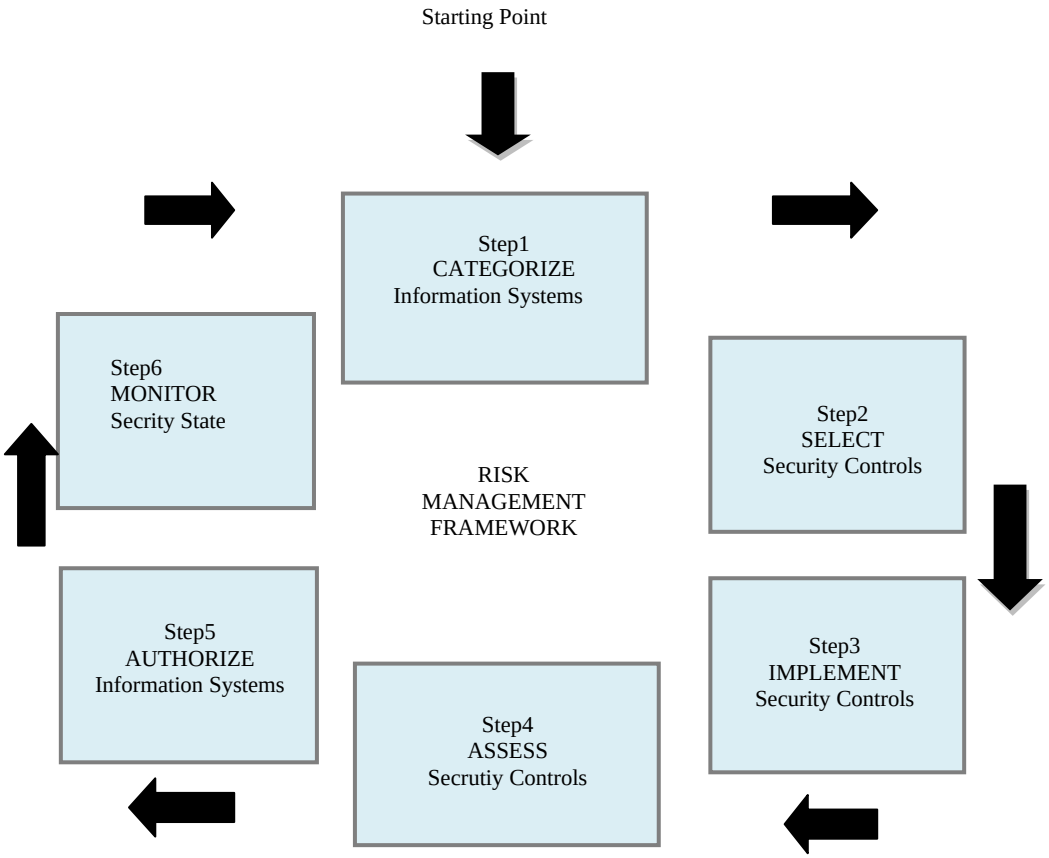

Fig.1: IT Security Risk Management of U.S. Federal Information Systems (From NIST SP800-37)

Class Determination is to determine the security protection class of an information system based on the importance of the information and the system, and the degree of harm to national security, social order, public interest, and the legal rights of citizens, legal entities or other organizations when the system is damaged. The process of class determination is the recognition process of the important information asset by the government. Generally, information risk evaluation relies on the information system itself to recognize such asset. With the progress in information technology, governmental affairs, social order maintenance and daily lives of regular citizens become more and more dependent on computer information systems. The application scope of an information system, is not limited to its own existence anymore, but rather expands to the entire society. It is related to national security, public interest, social stability and legal rights of citizens and organizations, thus a functional information system has a social relevance, and damages to it would impact national security, social order and people's daily lives. Therefore, from a national security point of view, it is critical to identify the information assets that are important to the country. Class determination is a pre-requisite for information security supervision, inspection and follow-up. Through class determination, it is possible for governmental information security agencies to keep track of important information or an information system, such as where it is located, who is operating it, and how important is the system. This will provide detailed fundamental information for national information security risk management. It is important because risk control and management requires deep knowledge of the managed assets.

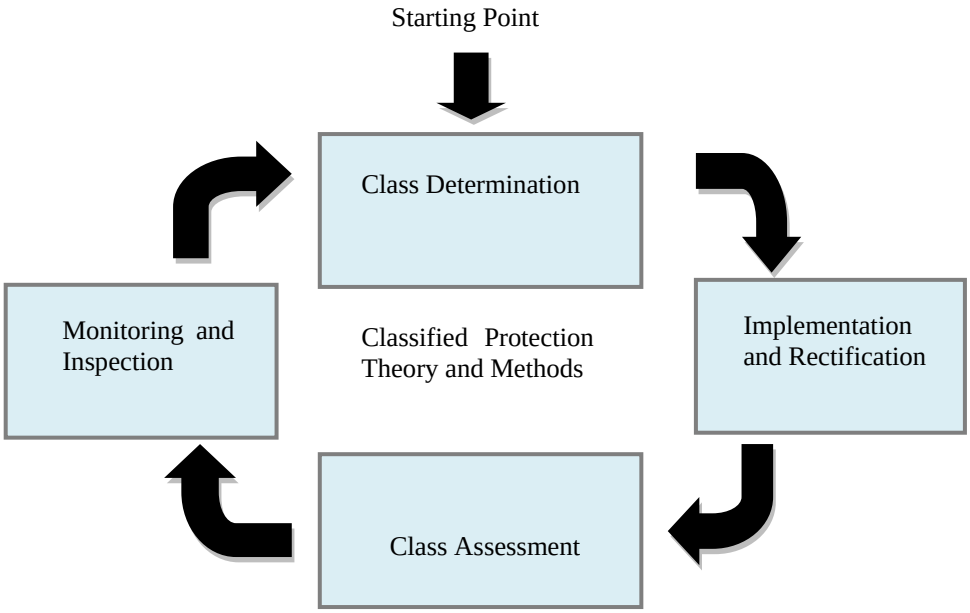

Fig.2: Information Security Classified Protection Implementation Process

Implementation and rectification is the control process for information system security risks. It involves selecting appropriate security control measures based on the security protection class of the system, and then implementing the selected control measures and management methods, to ensure that the information system has the protection capability corresponding to its security class. The purpose of risk management is not to guarantee zero risks, but rather to control the risk within an acceptable level. In “Basic Requirements for Information System Security Classified Protection”, the requirements for a system of a certain class is determined by the threat that a system with such class needs to defend against, and the capability of a system with this class (an information system’s security protection capability consists of defending capability and recovery capability). The requirements include 10 items from technology and management perspectives. The “Basic Requirements” documented minimum requirement for each item. The document also emphasizes on the combination of governmental supervision and the inherent security requirement of the system itself, and proposes to satisfy a basic security while striving for stronger security, giving a full consideration of the differences in the capability of risk aversion in different systems.

Class Assessment, Monitoring and Inspection are in fact processes to monitor the IT security risk, i.e. to confirm the effectiveness of the security control implementation. Different from the limited, system-focused security risk evaluation, Class Assessment is foremost a judging process for standard compliance. It relies on the national standards and industry standards of Information Security Classified Protection, adopts specific methods to determine the effectiveness of the implementation of security technology and management methodology of an information system, checks whether the implementation is correct, or the operation of the system is as predicted, or the security requirement is met. Class Assessment can not only identify inadequacies and hidden danger in the system for the operators, fully uncover the system risk and suggest implementation and rectification methods to satisfy standard compliance, but it can also determine whether the information security protection capability satisfies the requirements of national risk management and control. It comprehensively assesses whether the information system possesses the security protection capability required by the governmental regulations based on the classified protection rules, and whether the system is standard-compliant, thus it embodies a generalized national information security protection assessment.

Monitoring and Inspection is to continuously follow and monitor security status of the information system. It involves inspecting the changes of security condition and the operating environment of the system, and prompting the operators of the system to make improvement once

changes in threat have been detected.

Conclusion

Compared to the international information security risk management theory and practice, especially the US information risk management framework, it is obvious that the Information Security Classified Protection policy that we promote emphasizes the content of implementation, simplifies the technical details, and formulates four steps: class determination, implementation and rectification, class assessment and monitoring and inspection. Through this simplified process, we have created new thinking on critical information infrastructure protection, and fully conveyed the determination of our government in information security risk management and control. The policy also considers the supervising, monitoring and inspecting roles of governmental information security management agencies in the implementation steps, based on the characteristics of our information security management circumstances. Therefore, Information Security Classified Protection is fundamentally a national information security risk management and control process with Chinese characteristics.

As we enter the 21st century, more and more countries around the world are focusing research on how to combine the risk management theory and each country's own practical situation to create actionable plans for national information infrastructure protection. Critical infrastructure protection is not identical to information system protection. It is more focused on physical protection, network security and information analysis. How to elevate the theory and practice of Information Security Classified Protection, to create our own protection framework for nationally critical infrastructure of critical information infrastructure, is an important task ahead of us.

References

[1] Computer Information System Security Protection Ordinance of the People's Republic of China, State Council,1994.

[2] Supervision Methods for Classified Protection of information security, Ministry of Public Safety,2007.

[3] ISO/IEC 13335-1996，Guidelines for the Management of IT Security..

[4] ISO/IEC 27005-2005，Information Security Risk Management.

[5] NIST SP 800-39，Management of Information Security Risk.

[6] NIST SP 800-37， Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

[7] GB/T 22240-2008, Guide on Information system security protection class determination.

[8] GB/T 22239-2008, Basic Requirements for Information System Security Classified Protection.