DOI 10.15302/J-SSCAE-2016.06.021

Research on International ICT Supply Chain Security Management with Suggestions

Ni Guangnan[1], Chen Xiaohua[2], Shang Yanmin[3], Wang Hailong[1], Xu Kefu[3]

1. Institute of Computer Technology, Chinese Academy of Sciences, Beijing 100190, China
2. Chinese Academy of Cyberspace Studies, Beijing 100010, China
3. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract: Considering the reliance of a nation's critical infrastructure and key resources on information and communication technology (ICT), identifying and controlling the ICT supply chain risk has become important for protecting national security. As the forerunner of ICT supply chain management, the United States is rich in terms of its experience in enhancing the strategic position of the ICT supply chain, undertaking risk management, ensuring security of its software and hardware, and supervising its procurement. In addition, the European Union and Russia specifically strengthen the security management of the ICT supply chain. Based on the above research, this study provides certain suggestions on China's security management of the ICT supply chain.

Keywords: supply chain risk management; hardware supply chain; software supply chain; procurement security

1 Introduction

Information and communication technology (ICT) supply chain includes hardware and software supply chains, and generally comprise procurement, development, outsourcing, integration, and other sectors. The security of ICT supply chain largely depends on the intermediate links involving the purchaser, system integrators, network suppliers, and software and hardware vendors among others [1]. The ICT supply chain is the basis for all other supply chains, which is the "supply chain of supply chain" [2]. In the context of globalization of ICT procurement, the relationship between ICT supply chain security and national security is increasing in strength. Any link from raw material procurement, production, shipping, and delivery to final customers could have factors influencing ICT product security. From the perspective of the antagonistic nature of information security, international ICT product providers could possibility set malicious functions in the products, such as inserting malware in the software and/or hardware (including virus, Trojan, and spying software), which could lead to unexpected disruptions of critical ICT products and services.

Considering the reliance of a nation's critical infrastructure and key resources (CIKR) on ICTs, it has become a key subject to identify and control ICT supply chain risk.

The United States, the European Union, Russia, and other countries enhance the status of the security management of their ICT supply chain on both, the strategic and standard-setting levels. This paper studies the international ICT policies of security management of supply chains from the strategic and standard-setting level perspectives. Considering the aspect of security management practices of an ICT supply chain, this study discusses the current security management of ICT hardware and software, and further analyzes the safety in procurement of software and hardware from the United States. The purpose of this study is to draw lessons from the experiences of other countries, to provide suggestions for strengthening the security management of China's ICT supply chain, and to establish the security assessment system of the ICT supply chain.

Received date: 20 October 2016; **revised date:** 25 October 2016

Corresponding author: Ni Guangnan, Institute of Computer Technology Chinese Academy of Sciences, Academician. Major research field is multimedia technology. E-mail: ngn@public.bta.net.cn

Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)

Chinese version: Strategic Study of CAE 2016, 18 (6): 104–109

Cited item: Ni Guangnan et al. Research on International ICT Supply Chain Security Management with Suggestions. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.021

2 International ICT supply chain security management policies

2.1 Strategic positioning

The United States has focused on supply chain security for a long period of time. In 2008, the Bush Administration proposed the Comprehensive National Cybersecurity Initiative (CNCI) [3], where one of the key tasks was to develop versatile methods to execute global supply chain risk management (SCRM). In 2009, the Obama Administration presented that it was imperative to introduce new SCRM methods, in addition to merely condemning international suppliers of products and services. In 2011, the United States released the International Strategy for Cyberspace [4], which prioritizes negotiations between the government and the industrial sector to enhance supply chain security using high technology, in order to safeguard the cyberspace security.

The European Union, Russia, and China have increased the security of ICT supply chain to the level of a national security strategy. In the report entitled "Supply Chain Integrity", the European Union demonstrated that improvement of ICT supply chain integrity was essential for the economic development of a country, and thus, it was significantly valued by the private and public sectors [5]. The International Code of Conduct for Information Security was jointly delivered by Russia and China to the United Nations. It highlighted that all efforts should ensure the security of the ICT product and service supply chain to prevent other countries from taking advantage of their own resources, critical facilities, and core technologies, to weaken the autonomous control of developing countries over ICT products. It also aimed at preventing developing countries from political, economical, and social threat from other countries [6].

2.2 ICT supply chain risk management

2.2.1 United States National Institute of Standards and Technology

The United States National Institute of Standards and Technology (NIST) is responsible for developing the standards and guidelines, as well as testing and measuring the index for the protection of non-national security federal information and communication infrastructure. It has cooperated with the shareholders of private and public sectors for the research and development (R&D) of ICT SCRM tools and indexes, and the related guidelines on reduction measures and execution methods.

2.2.2 ICT SCRM programs and resources

(1) CNCI#11

The ICT SCRM program of the NIST began in 2008, when it initiated the development of ICT SCRM practices for non-national security information system, in response to the Comprehensive National Cybersecurity Initiative (CNCI) #11, "Develop a multi-pronged approach for global supply chain risk management." The CNCI#11 has provided SCRM practices for federal information systems and organizations. The CNCI#11 Working Group 2 (WG2) is responsible for highly evaluating threats, vulnerabilities, and consequences with regard to purchase decision-making, and identifying and mitigating the risks of resources throughout the product and service life cycle to improve SCRM.

(2) NIST Special Publication 800-161 (SP 800-161)

The draft of NIST SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations [7] provides a guide for the federal agencies to develop the appropriate policies, processes, and controls to effectively manage ICT supply chain risk. NIST SP 800-161 provides a template for developing ICT SCRM plans that address the entire system development life cycle. The template specifies a set of processes to evaluate and manage supply chain risks, lists the applicable threat events, and provides a risk framework to evaluate threat and confirm reduction measures (namely, the evaluation method of an event correlation and its potential impact). These procedures are incorporated into the risk management process (architecture, evaluation, response, and monitoring) of the NIST SP 800-39 [8] and are executed as part of the complete risk management activities of federal agencies.

(3) NIST Interagency Report 7622 (IR 7622)

NIST IR 7622: National Supply Chain Risk Management Practices for Federal Information Systems [9] is a guide on networks SCRM, which is drafted by the NIST to eliminate the life-cycle supply chain risks of high-impact joint information systems during procurement, development, and operation, and to introduce specific ICT SCRM practices.

The second version of the NIST IR 7622 (NIST 7622-2) illustrates the application of SCRM in ICT and provides a set of practices that can be directly applied to procurements and contracts that are categorized at the Federal Information Processing Standards (FIPS) 199 high-impact level. The stakeholders in the NIST 7622-2 include information system procurement parties, procurement teams, an information system security personnel, and engineers in-charge of information system delivery. NIST IR 7622-2 covers all links providing product and information security services to the government and business organizations.

An integrated SCRM procurement process is analyzed in the NIST IR7622-2. Fig. 1 represents the ICT SCRM procurement process. Considering these information systems categorized at the FIPS199 high-impact level, the ICT SCRM should be directly included in the procurement process to analyze potential supply chain risks and implement additional security controls and/or SCRM practices as needed. For information systems categorized at the FIPS199 moderate-impact level, authorized agencies should take risk-based decisions on whether the ICT SCRM is

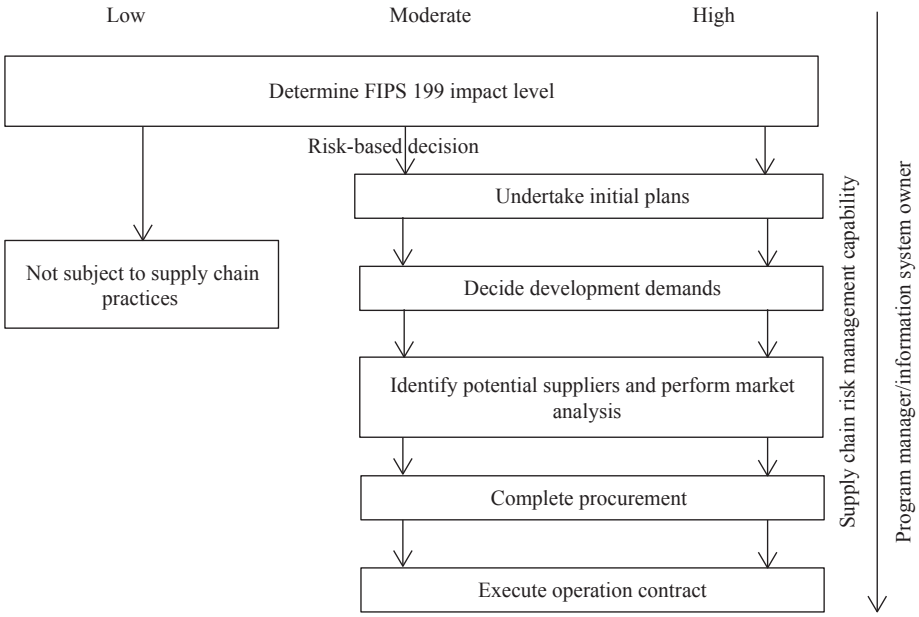

Fig. 1. ICT SCRM procurement process.

required; and for information systems categorized at the FIPS199 low-impact level, implementing ICT SCRM is not required.

3 International ICT supply chain security management practices

3.1 Hardware/software supply chain security management

3.1.1 Hardware supply chain security

An ICT hardware supply chain refers to a series of processes from ICT hardware procurement, design, manufacturing and assembling, and allocation to maintenance and treatment.

The length, complexity, and vulnerability of ICT hardware supply chains have correspondingly increased over the last few years. Currently, government departments globally have begun to consider threats produced by the ICT hardware supply chain to their ICT systems. During the exchange of resources between the ICT hardware supply chain system and the external environment, and in the coordination and cooperation of supply chain participants, there exist various internal and external uncertainties. External risks include natural disasters, terrorist incidents, and emergencies. Internal risks include supply disruption, such as manufacturing and delivery disruption caused by attackers, incorrect transport routes or delivery delays, incorrect orders (such as incorrect quantities or items), and inferior manufacturing quality (e.g., hardware-based threats).

Currently, hardware SCRM is primarily undertaken for three important hardware risks, which are Trojan, malicious firmware, and hardware forging.

3.1.2 Software supply chain security

While paying attention to the security of the hardware supply chain, the security of the software supply chain should not be ignored as no supply chain can be used without software. The software supply chain can influence every aspect of the delivered system. When the supply chain participants have access to the final software code or system, risks endangering the software supply chain security could exist. The supply chain participants could include suppliers who code, enhance, or change product or system contents, distributors, and transporters [10].

Risk evaluation is a basic aspect of risk management. Software supply chain risk evaluation involves, from a risk management perspective, analyzing the threats and vulnerabilities of the software supply chain in a systematic manner through scientific methods and means, evaluating the possible influence on the whole supply chain or losses that individuals could suffer in cases of risks, and establishing corresponding and verification measures to prevent threats. Among the limited methods of risk evaluation for software supply chains, the most commonly used is the risk evaluation method proposed by the Software Engineering Institute (SEI) of the Carnegie Mellon University. Fig. 2 describes a prototype of SEI evaluating systematic software supply chain risks using the risk-driven method.

3.2 Procurement security management

3.2.1 Government regulations

In the late 1990s, the Unites States realized the severity of government procurement issues. Presidential Decision Directive 63 issued by the Clinton Administration on May 22, 1998, stated that information security should be confirmed in large procurement tasks. During the Bush Administration, this issue was further specified. In 2002, the Bush Administration began to draft a national security strategy, which further specified the procure-

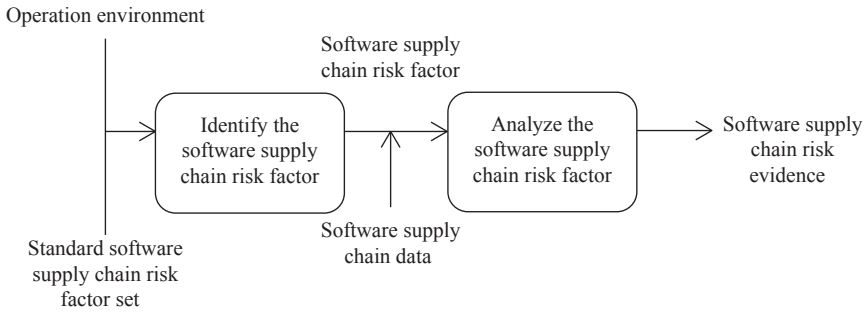

Fig. 2. Software supply chain risk evaluation.

ment steps, processes, and related standards. In December 2008, before Barack Obama took charge of his office, the United States Center for Strategic and International Studies (CSIS) released an advisory report titled "Securing Cyberspace for the 44th Presidency" [11], pursuant to which several important suggestions were made to the new president. The suggestions included enhancing security using procurement principles, and cooperation between the government and the industrial sector in developing and undertaking security measures.

In the first half of 2016, the European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC), and European Telecommunications Standards Institute (ETSI) included new requirements to access ICT products and services from Europe, and these were applicable to government procurement, highlighting this for the first time in Europe through legislation. The new requirements expected government departments and other public agencies to assure improved accessibility to services, software, electronic equipment, and other products, when purchasing ICT products and services.

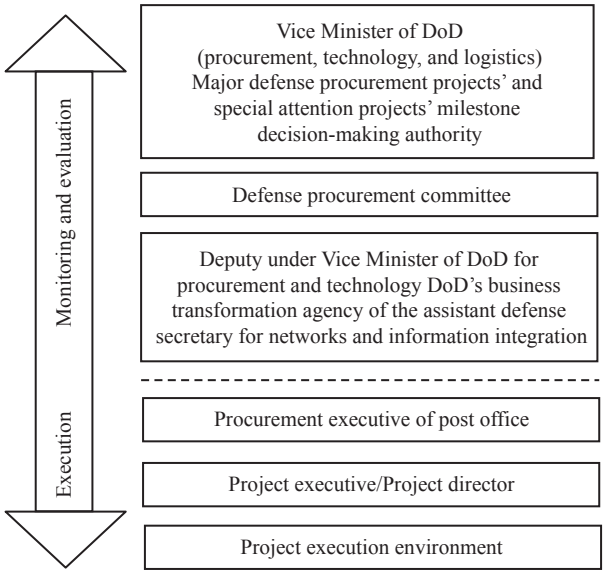

Fig. 3. Different types of ICT procurement projects.

3.2.2 Examples of national defense procurement security processes

The procurement of ICT products and services is divided into two categories, national defense procurement and corporate procurement. Among these, the requirements for national defense procurement are higher. The following points provide a brief introduction to the management and procurement systems of the United States' military in the secure procurement of ICT products and services, which could provide insights for China in its ICT national defense procurement.

(1) Management of ICT procurement

Procurement undertaken by the DoD adopts the management mode of a real-time combination of unified DoD leadership and decentralized execution of military services. Unified leadership refers to establishing the position of deputy secretary of defense for procurement, technology, and logistics, who is responsible for military ICT R&D and procurement. Decentralized execution is adopted to perform class and level management in terms of the importance and expense of ICT projects. Considering the class of procurement of ICT projects, the deputy secretary of defense for procurement, technology, and logistics assigns the corresponding level milestone decision-making authority, in order to monitor the decisions undertaken (Fig. 3).

(2) Procurement system of ICT

The United States DoD has established the DoD's ICT procurement system with three branches that work in coordination to complete the ICT procurement procedure for military products. These three branches, which are mutually supported, interacted, and restrained during the procurement of weapons for the United States, are as follows: planning, programming, budgeting, and execution process; joint capabilities integration and development system; and defense acquisition system [12].

4 Suggestions to establish a security evaluation system for ICT supply chain in China

Considering China's inferior ICT supply chain, according to the National Security Law of the People's Republic of China, strengthening the security assessment and management of ICT

supply chain and establishing an ICT supply chain security assessment system are the most urgent tasks in the national cybersecurity review. Based on the analysis of the current situation of international ICT supply chain security management, this study provides suggestions for security management and assessment of China's ICT supply chain.

(1) Enhance security management of the ICT supply chain at a national strategic level

The suggestions for enhancements include emphasizing supply chain security management at a national strategic level and promoting research and development of corresponding systems and standards; researching core technology related to ICT supply chain security management; considering security management of the ICT supply chain as a legitimate need for guaranteeing national cybersecurity; and ensuring that it is easily accepted by the international community. As the establishment of the ICT supply chain security management system is an international practice, a national ICT supply chain security assessment system should be established in China as well.

(2) Incorporate the ICT supply chain assessment into the cybersecurity review

Some suggestions include strengthening the cybersecurity review for the ICT supply chain; and supervising the design, research, development, manufacturing, production, distribution, installation, operation, maintenance, procurement, and other aspects of ICT products and services. Incorporating ICT supply chain assessment into cybersecurity review can clarify that cybersecurity censorship is not targeted at specific countries or regions, and can alleviate the concerns and suspicions of foreign parties that consider the system as a trade barrier.

(3) Formulate laws and regulations for ICT supply chain security assessment

China should formulate and improve national policies, laws, and standards; and define the responsibilities and obligations that the parties should consider in the security assessment of the ICT supply chain. ICT supply chain security assessment involves the application and coordination of a number of laws, including technology import and export control, and commercial password control and certification, which are the most closely related laws to the ICT supply chain security assessment. However, these laws and regulations need to be modified to suit cybersecurity review.

(4) Organization of the ICT supply chain security assessment

China should change the decentralized security assessment approach of the ICT supply chain by establishing a unified assessment agency. The assessment agency could be an existing management department related to the ICT supply chain security, or a newly established assessment agency, which would be responsible for the unified deployment and coordination of security management and review of the ICT supply chain.

(5) Establish procedures for the ICT supply chain security assessment

The assessment agencies should draw lessons from the existing international information security assessment systems and then assess the security performance of ICT products and services by using a criterion of supply chain security assessment. The assessment procedures include assessment preparation, a primary assessment, a secondary assessment, periodic assessment, and a re-certification assessment stage.

5 Conclusions

Considering the features of the current international ICT supply chain security management, it is necessary for China to strengthen its strategic research on security management of the ICT supply chain, to formulate common security assessment standards of the ICT supply chain, and to enhance the link between security assessment of the ICT supply chain and the existing information security systems.

References

[1] Boyson S, Rossman H. Developing a cyber-supply chain assurance reference model [R]. Maryland: Supply Chain Management Center (SCMC), Robert H. Smith School of Business University of Maryland, 2009.

[2] Booz Allen Hamilton. Managing risk in global ICT supply chains: best practices and standards for acquiring ICT [R]. McLean, Virginia: Booz Allen Hamilton, 2012.

[3] The comprehensive national cyber security initiative [EB/OL]. (2008-01) [2016-10-12]. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[4] Schmidt H A. International strategy for cyberspace [R]. Washington, DC: White House, 2011.

[5] Cadzow S, Giannopoulos G, Merle A, et al. Supply chain integrity: an overview of the ICT supply chain risks and challenges, and vision for the way forward (2015) [R/OL]. (2015-09-11) [2016-10-15]. https://www.enisa.europa.eu/publications/sci-2015.

[6] The Embassy of the People's Republic of China in New Zealand (Cook Islands, Niue). China, Russia and other countries submit the document of international code of conduct for information security to the United Nations International code of conduct for information security [EB/OL]. (2011-09-12) [2016-10-15]. http://www.chinaembassy.org.nz/eng/zgyw/t858978.htm

[7] Boyens J, Paulsen C, Moorthy R, et al. NIST special publication 800-161: supply chain risk management practices for federal information systems and organizations [S]. Gaithersburg: National Institute of Standards and Technology, 2015.

[8] Ross R S. NIST special publication 800-39, managing information security risk: organization, mission, and information system view [S]. Gaithersburg: National Institute of Standards and Technology, 2011.

[9] Boyens J. NIST IR7622: Notional supply chain risk manage-

ment practices for federal information systems [S]. Gaithersburg: National Institute of Standards and Technology, 2012.

[10] Simpson S, Reddy D, Minnis B, et al. The software supply chain integrity framework: defining risks and responsibilities for securing software in the global supply chain [S]. SAFECode, 2009.

[11] Langevin J R, McCaul M T, Charney S, et al. Securing cyberspace for the 44th presidency: a report of the CSIS commission on cybersecurity for the 44th presidency [R]. Washington, DC: Center for Strategic and International Studies, 2008.

[12] Chadwick S H. Defense acquisition: overview, issues, and options for congress [R]. Washington, DC: Congressional Research Service, the Library of Congress, 2007.