Study on Architecture-Oriented Information Security Management Model for Using Mobile Devices Control

Wei-ming Ma
Cheng Shiu University, Taiwan

The popularization of mobile devices has caused considerable impact on the security of the military of the Republic of China. The military barrack-areas have long been faced the control of mobile devices four issues: the lack of accurate use of resources, the lack of protection of the mobile device from the overall point of view, the unclear division of responsibility among specialized agencies, and unclear members’ responsibilities for their own duties. This study applies the structure behavior coalescence (SBC) methodology to integrate the organizational structure of the participating management and control units with effective management behaviors in a visualized and useful manner. The units can effectively communicate with each other and solve the four issues faced by the military barrack-areas for the control of mobile devices. This research fulfills improving the lack of control of the military mobile devices by using of management resources effectively and the establishment of mobile devices management with the overall concept, and strengthening the rights and responsibilities and information security awareness, through the logical verification and enterprise interview results.

Keywords: information security management, structure behavior coalescence, mobile devices, Military Army

Introduction

In this chapter, the study background and motivation, study goal, and study method for information security of using mobile devices control are described.

Study Background

The Republic of China’s Military Army (hereinafter referred to as the “Military Army”) promulgated controls on the use of mobile devices. The system only opened non-camera Internet-enabled mobile phones (i.e., the second-generation, 2G mobile phones) due to the suspension of 2G mobile phone signals and Hong Jun’s disciplinary events in June 2013. After Hong’s case, the Military Army turned positive on the control of mobile devices. Since the beginning of New Year’s Day in 2014, it began to pilot the regional control of volunteers as an open-use mobile device. It opened the use of compulsory military service from the New Year’s Day in 2015 and has fully promoted since July 2016. The mobile device management (MDM) program is installed to seek a
balance between the convenience of mobile devices and the security protection of the Military Army barrack-areas (hereinafter referred to as barrack-areas). Since the Military Army controlled the opening of mobile devices, related research and related practices have been continuously implemented and improved. However, there are still many cases of leaks through the installation of programs, gate control, barrack-areas restricted settings, irregular security inspections, and regular information security education practices. This shows that there are still loopholes in information security management in the current mobile devices use tube production method, which still needs improvement.

All mobile phones of the Military Army use control measures, but newspapers on the media can still be found repeatedly in the newspaper media because mobile devices transmit sensitive photos and official documents. The overall security protection of mobile devices by the military army is still not mature enough. It only pays attention to the implementation process but neglects the clear understanding of the structure of the participating management units, resulting in a serious separation of the structure and process. The command and control relationship between the vertical units is not clear, and there is a lack of management communication between horizontal mobile devices, failure to integrate management resources, effective use, and inappropriate execution behaviors that need to be improved. In addition, since the opening of the mobile device, the Military Army has purchased its own mobile devices for combat training, disaster relief, and drill exercises. From this point of view, the relevance of mobile devices to the Military Army will only deepen. Surrounding issues, such as education and training, leak prevention, and control of mobile devices deserve the management to pay more attention to and implement the management system.

Motivation

The goal of this study will thoroughly explore the four issues that the Military Army has faced for the control of mobile devices for a long time, and have sought to propose improvements:

1. Resources have not been used exactly: At present, the Military Army has invested considerable resources. However, because some departments do not understand the characteristics of various resources, they cannot use resources effectively and create loopholes in information security protection.

2. The lack of an overall concept: Each department only provides professional insights for its own professional sections and is trapped in professionalism. It has not been fully reviewed, resulting in the lack of an overall concept of information security protection.

3. Unclear division of human resources: Because process-oriented mobile device management methods fail to explain in detail what each member should do and how to do it will lead to easy focus on some of the personnel and increase the workload. The rest of the staffs will stand idle while doing nothing, causing wasted human resources and uneven distribution of resources.

4. Members are not clear about their duties and responsibilities: If members do not know exactly what to do, they should coordinate with those departments. When the information security incident occurs, the strain will depend entirely on personal experience and fail to comply with relevant regulations.

Study Goal

This research uses the structure behavior coalescence methodology to integrate the organizational structure of the participating management units with effective information security management behaviors and to visually solve the four problems faced by the Military Army for the control of mobile devices and achieve effective improvement:
(1) The effective use of management resources: Through the unity of structural and behavioral methodology, the overall organizational structure, the overall observation and implementation of standard operating procedures, and the effective use of management resources to prevent information security protection loopholes.

(2) Establishing the overall concept of mobile device management: Understanding the overall management function or behavior of mobile device management through the six structure behavior coalescence diagrams, the vertical command system to effectively communicate directives, horizontal effective support communication, comprehensively reviewing again, and proposing overall effective mobile device management the concept of information security protection to improve the leakage of sensitive information.

(3) Clear professional division of human resources control behavior: As the process-oriented mobile device management method separates the organizational structure and management behavior, each department has unclear powers and responsibilities, and it is unable to display the professional knowledge of each unit. The structure behavior coalescence methodology can be visualized. The way helps the military units to specify the duties of each member of the business, the members know what to do, know how to do, and make full use of resources to diversify the workload and the effective use of human resources.

(4) Strengthen the recognition of duties and responsibilities and information security: Through interviews, the structure behavior coalescence methodology allows each member to know exactly the information security regulations to be complied with. All departments fully communicate and coordinate and will handle information security incidents, the inheritance of knowledge, and experience.

Study Method
This research adopts the structure behavior coalescence methodology proposed by W. S. Chao, W. Chao, and H. Chao (2008). Through the structure behavior coalescence model, the six golden rules will be used to conduct a holistic analysis of the Military Army’s mobile device management practices. After the analyzing and modeling, the “architecture-oriented enterprise mobile device information security management model” was established.

Literature Review
This chapter summarizes the relevant domestic and foreign scholars’ knowledge of the relevant papers about this study, including information security management system, the structure behavior coalescence methodology, and the Military Army’s computer emergency processing and contingency plans, are described briefly.

Information Security Management System
The definition of information security is: “preservation of confidentiality, integrity and availability of information” (ISO, 2018). Confidentiality is a property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Integrity is a property of accuracy and completeness. Availability is property of being accessible and usable upon demand by an authorized entity. ISO 27000: 2018 information security management system (ISMS) specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. The adoption of the ISMS is a strategic decision for the organization. The establishment and implementation of the organization of the ISMS influenced by its needs and objectives, security requirements, organizational processes adopted, and the size and structure of the organization; all influencing factors are
expected to change over the time. The information security management system maintains information by using risk management processes. Confidentiality, integrity, and availability allow stakeholders to believe that the risk has been appropriately managed to generate confidence. Importantly, the ISMS as part of the organizational process should be integrated with the organizational process and the overall management structure. And information security is included in the design of processes, information systems, and control measures. That the ISMS will be implemented in accordance with the needs of the organization can be reached. Internal or external parties use ISMS to assess the organization’s ability to reach their own information security requirements matters.

The organization should identify external and internal issues that are relevant to its objectives and affect its ability to achieve the expected results of the ISMS. The organization shall determine: a) the interest groups related to the ISMS; and b) the needs of interested parties related to information security. The organization shall determine the boundaries and suitability of the ISMS to establish its scope and provide it with documented information. Senior managers should demonstrate leadership and commitment to the ISMS and establish information security policies. Senior managers should ensure that the responsibilities and authorizations of information security related roles are distributed and communicated. The control and human resources for mobile devices related to the control measures in Appendix A of ISO/IEC 27001:2013 (ISO 27001 Standard) ISMS Requirements related to this study:

A6.2 Mobile devices and teleworking in A6. Organization of information security: To ensure the security of teleworking and use of mobile devices, a policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.

A7 Human resource security:

A7.1 Prior to employment: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. A7.1.1 Screening: Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations, and ethics and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. A7.1.2 Terms and conditions of employment: The contractual agreements with employees and contractors shall state their and the organization’s responsibilities for information security.

A7.2 During employment: To ensure that employees and contractors are aware of and fulfil their information security responsibilities. A7.2.1 Management responsibilities: Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. A7.2.2 Information security awareness, education and training: All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. A7.2.3 Disciplinary process: There shall be a formal and communicated disciplinary process in place to act against employees who have committed an information security breach.

A7.3 Termination and change of employment: To protect the organization’s interests as part of the process of changing or terminating employment. A7.3.1 Termination or change of employment responsibilities: Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor, and enforced.

According to the latest development in science and technology, the ISMS is continuously revised through the PDCA (Plan-do-check-Act) model, so that the revised ISMS can be close to the desired goals of the
organization. The Ministry of Defense and its affiliates also adopted the ISO27000: 2018 standard. According to the standard risk assessment method, the ISMS was developed for the appropriate military units through the PDCA model. The national security policy clearly states that the goal of the security and security system is to use the methods outlined in ISO 27001 for risk assessment to develop risk tolerance criteria and identify acceptable risk levels. The selected risk assessment method must ensure risk assessment and produce comparable and reproducible results (ISO, 2018).

**Structure Behavior Coalescence Methodology**

Chao (2013) studied the five process-oriented enterprise architecture problems: lack of organization structural support, organizational behavior cannot meet the organizational structure, fall into a functional-oriented, cannot control the enterprise’s multiple perspectives, and cannot demonstrate the corporate hierarchy. The exploration of the current operations of the Military Army’s mobile device management system is mainly process-oriented. However, according to the actual operation of a comprehensive consolidation, there have been problems, such as the lack of accurate use of resources, the lack of an overall concept, unclear division of human resources, and unclear members’ responsibilities for their own duties. Sufficient to see the process-oriented and cannot really prevent the closure of security breaches.

This study was based on Chao et al. (2008) who proposed the structure behavior coalescence (SBC) methodology. Six golden rules, namely, architecture hierarchy diagram (AHD), framework diagram (FD), component operation diagram (COD), component connection diagram (CCD), structure behavior coalescence diagram (SBCD), and the interaction flow diagram (IFD) are used to build enterprise architectural models. The six diagrams are described as followings:

1. **Architecture hierarchy diagram (AHD):** At this stage, it is to disassemble a complete system to a process that cannot be disassembled. As shown in Figure 1, a system may contain component A and subsystems, and the subsystem can still be disassembled to Component B and component C, so the subsystem is also known as the aggregated system. For example, a common military weapon is a rifle. A rifle is a system. A rifle can be disassembled into a gun body, a butt, an ammunition, and a bolt mechanism. Since the demolition is sustainable except for the magazine, the magazine is regarded as a component. The rest parts of rifle are considered as a polymerization system; the buttock is disassembled into a buttstock and a strap. Since the buttock and strap are no longer disassembled, they are regarded as components and the demolition of the buttock is completed. It is worth noting that in the AHD but the “view” is emphasized. Through the point of view, you can understand the relationship between systems, aggregation systems, and components.

2. **Framework diagram (FD):** FD is mainly used to display the components in each layer. It is noteworthy that in the FD, all the components in a layer are “components” without any sub-components (system also known as aggregating system). Because of its non-hierarchical relationship in FD, it allows readers to quickly and clearly understand that the hierarchy is composed of those components.

3. **Component operation diagram (COD):** According to Chao’s (2012) argument, the operations must be completed using the operation formula. The operation formula includes: a) operation name; b) input parameter; and c) output parameter name and data type; the parameter direction refers to that the component is the input parameter, and vice versa is the output parameter. It is worth noting that a component may not have only one operation name. The black part of component A in the component operation diagram organized in this study is the operation name; in addition, the input parameters and output parameters should be drawn according to the
actual conditions, but they do not necessarily exist. For example, components in this study example have only input parameters and no output parameters.

(4) Component connection diagram (CCD): The CCD of the components is the relationship between the operation and linkage relations between the narration component and the component or between the component and the external environment. The example actor in this study is the external environment. The black line is the operation. The linkage relationship is as follows: the external environment (the agent) moves through the operation A and the component A; the component A links through the operation B and the component B; component A is linked to component C through operation C.

(5) Structure behavior coalescence diagram (SBCD): At this stage, further operations that are linked to each other are chained into behaviors. Taking the example of this study, the operation A between the external environment (actor) and the component A and the operation B between the component A and the component B constitute the linkage, thus forming the behavior A; the operation A between the component A and the component C causes operation C linkage, so behavior B is formed. The external environment does not necessarily have only one item, and the behavior formed by the linkage between the external environment and components may not be the only one.

(6) Interaction flow diagram (IFD): The IFD is used to explain the “behavior” of the SBCD. How many behaviors in an architecture modeling process should have multiple interactive flowcharts? In other words, an IFD is only used to explain the relationship between elements in an action. Taking the example behavior A of this research as an example, the external environment (behavior role) and component A form a linkage through operation A; component A and component B operate through operation B. The input parameter arrow indicates the direction in which the operation is performed, and the operation point black point indicates the element that accepts the operation trigger. If the operation receiver is reversed and there is an output parameter, a feedback operation is generated after the component representing the receiving end processes the operation sent by the component sending end. This feedback operation may not be sent back to the original sender but may be sent to the corresponding element depending on the actual condition. This element may be any component within the behavior or may be directly transmitted back to the external environment. It is also possible that behavior will not happen.

The molding process of the SBC structure is based on the six gold laws to complete the molding process one by one. To facilitate the understanding of the molding process, this study is compared with the graphic illustrations of Chao et al.’s (2008) six gold laws on the teaching website and this study, as shown in Figure 1.

Ma (2017) used the Structural Behavioral Coalescence methodology to study the information security Internet of Things (IoT) system architecture and recommends that IoT sensor vendors implement security certifications, database auditing, and other results. Ma (2014; 2016) researched architecture-oriented information security risk management model, which effectively improve the company’s proper allocation of resources, reduce the complexity of information security risk management, and reduce risk. Ma (2014) studied the architecture-oriented implement of the Personal Information Protection Act on an university campus to introduce the model of personal information protection and provided the information unit with a clear organization for the integration of human resources distribution and auditing. Fully explaining the methodological theory of structural behavior can effectively solve the information security issues that companies are concerned about.
Figure 1. Six golden rules of SBC architecture molding. Source: Chao (2008).
Taking the architecture-oriented methodology as the research method, we explored the practice of controlling and controlling mobile devices in the barrack of the Military Army. Obviously, process-oriented standard operation process focuses on the behavior and technical level. Although the discussion mentioned personnel department, security department, access control unit, and so on, the mode of operation is still based on process orientation and it is impossible to see the correlation between departments. In the management of military barracks, the most difficult variable to control is personnel. Therefore, it is very important for people’s “management”. It is necessary to strengthen the management of users and supplement information technology management; rather than using technology as the most important means of management. The current mobile device controlling method has considerable changes in various regulations, external environment, hardware equipment, and organizational structure. Therefore, this study will use the architecture-oriented mobile device management and control method to set the research focus on the essence of management. It is necessary to conduct a comprehensive review of the organization, system, technology, correct use, and control of mobile devices in the barrack.

Mobile Device Management and Control of Hardware and Technology

The mobile device management and control of hardware and technology for the Military Army include three technologies: mobile device MDM, mobile monitor, and mobile device frequency masker. Hayes (2014) studied a cell phone jammer, a device that prevents cellular telephone users from connecting with other cellular telephones by blocking all radio signals. Mobile phone jammers are devices that prevent mobile phone users from connecting with other mobile phones. A mobile phone jammer transmits a signal on the same frequencies as cell phones for preventing all cell phone communication within a given area. The cell phone jammers are widely used in Europe and they are illegal in the US (Gregg et al., 2006).

Architecture-Oriented Information Security Management Model for Using Mobile Devices Control Design

The SBC methodology to design an architecture-oriented information security management model for using mobile devices control (AOISMMUMDC) includes: architecture hierarchy diagram, component diagram, component operation diagram, component connection diagram, structure behavior coalescence diagram, and interaction flow diagram.

Architecture Hierarchy Diagram

Any management model can be illustrated by an architecture hierarchy diagram (AHD) for the structure of a system’s decomposition and combination to understand complex systems easily. AHD is obtained after finishing the architecture construction. Figure 2 shows an AHD of AOISMMUMDC. In Figure 2, AOISMMUMDC composed of organization layer, application layer, data layer, and technology layer. Organization layer is composed of logistics department, personnel department, information department, accounting and statistics office, political general department, legal affairs office, and public security office. Application layer is composed of financial management graphical user interface (GUI), information management GUI, personnel management GUI, and logistics management GUI. Data layer is composed of logistics management database, personnel management database, information management database, document database, and financial management database. Technology layer is composed of mobile device MDM, mobile monitor, and mobile device frequency masker, as shown in Figure 2.
Component Diagram

Collection of non-aggregated systems or structure elements of architecture hierarchy diagram become the component diagram. From Figure 3, there are four layers: organization layer, application layer, data layer, and technology layer. The organization layer includes seven units: logistics department, personnel department, information department, accounting and statistics office, political general department, legal affairs office, and public security office. The application layer includes four graphic user interfaces: financial management GUI, information management GUI, personnel management GUI, and logistics management GUI. The data layer includes five databases: logistics management database, personnel management database, information management database, document database, and financial management database. The technology layer includes three technologies: mobile device MDM, mobile monitor, and mobile device frequency masker, as shown in Figure 3.

Figure 2. Architecture hierarchy diagram of AOISMMUMDC.
Component Operation Diagram

For a system, we use component operation diagram (COD) to demonstrate all components operations. COD is the third fundamental diagram to achieve structure behavior coalescence. The structure components that provide many operations through the interface or work content of the structure components with input or output parameters are called a COD. Input parameter of the service is denoted by an arrow symbol directed to structure element. Output parameters of the operation are denoted by an arrow symbol leave the component. Based on the collection of literature, standard operation procedure (SOP), sorted out the structure components step by step, and operations of 19 components were obtained for the AOISMMUMDC, as shown in Figure 4.

Component Connection Diagram

A component connection diagram (CCD) connects operations between the various components in accordance with its priorities. CCD is obtained after the analysis phase is finished. We use the CCD to describe how the components and actors (in the external environment) are connected within the AOISMMUMDC. CCD is the fourth fundamental diagram to achieve structure behavior coalescence. Rectangular frame is the system
boundary; the logistics department, personnel department, information department, accounting and statistics office, political general department, legal affairs office, and public security office are the external environment. If the operation or service provided by the component is not used, it must be deleted, as shown in Figure 5.

Figure 4. Component operation diagram of AOISMMUMDC.
Figure 5. Component connection diagram of AOISMMUMDC.
Structure Behavior Coalescence Diagram

The major purpose of adopting the architectural approach, instead of separating the structure model from the behavior model, is to achieve one single coalesced model. In Figure 5, systems architect can see that systems structure and systems behavior coexist in the SBCD. That is, in the SBCD of the AOISMMUMDC, systems architect not only sees its systems structure but also sees its systems behavior simultaneously.

From the component diagram and component operation diagram, we further derive out 10 behaviors of the AOISMMUMDC model: (1) application behavior, (2) rewards and punishments behavior, (3) promulgated plan behavior, (4) annulment behavior, (5) change behavior, (6) procurement behavior, (7) account creation behavior, (8) emergency response behavior, (9) masking signal behavior, and (10) entry access control inspection behavior, as shown in Figure 5 and Table 1.

SBCD is the structure behavior coalescence diagram we obtain after the architecture construction is finished. Figure 5 shows a SBCD of the AOISMMUMDC, in which interactions among the organization layer (logistics department, personnel department, information department, accounting and statistics office, political general department, legal affairs office, and public security office), the application layer (financial management GUI, information management GUI, personnel management GUI, and logistics management GUI), data layer (logistics management database, personnel management database, information management database, document database, and financial management database), and technology layer (mobile device MDM, mobile monitor, and mobile device frequency masker) shall draw forth 10 behaviors (application behavior, rewards and punishments behavior, promulgated plan behavior, annulment behavior change behavior, procurement behavior, account creation behavior, emergency response behavior, masking signal behavior, and entry access control inspection behavior). In other words, these 10 behaviors together provide the overall behavior of the AOISMMUMDC. The description of each behavior is as follows, as shown in Figure 6 and Table 1.

1) Rewards and punishments behavior: To truly achieve the effect of punishing errors and promoting goodness, the chief of information security officer (CISO) submits rewards and penalties to the department of information on the merits of assistant clerk and staffs. After receiving recommendations form of award and punishment from CISO, then it is confirmed that the quotation cited in the rewards and punishments proposal is unquestionable; they will recommend rewards and punishments to the Ministry of Personnel. After receiving the rewards and punishments of the CISO, the Ministry of Personnel conducted a review of the articles. After confirming that there was no doubt, the Ministry of Personnel Management will use the personnel management GUI to carry out citations and information on rewards and punishments. After notifying, the information will be stored in the personnel management database. After the data are stored, the reward and punishment order are sent to the employee.

2) Promulgated plan behavior: After the information security officer (ISO) promulgating the latest mobile device management measures and SOPs according to the superiors, the ISO shall create plans for the applicable barrack areas in accordance with the characteristics of the areas and submit the plans to the Information Department. After receiving the plan submitted by the ISO, the information department uploads and saves it to the information management database using the information management GUI, and then sends the plan to the employee’s mailbox by e-mail servers.

3) Application behavior: Newly arrived assistant clerk or staff submits a mobile device application form to the information department. After receiving the mobile device application form, the information department
uses the personnel management GUI to confirm the identity and confirms that the applicant is indeed a member of the department. The department of information then uses the information management GUI to submit the applicant’s submission-related data for fabrication and storage in the information management database. After the storage being completed, the information department uses the information management GUI to create a mobile device control label and sends to individual after the production being completed.

(4) Annulment behavior: Before retiring, the employee submits the cancellation application form and submits it to the CISO together with the mobile device control label used. After receiving the application form, the information department uses the personnel management GUI to confirm that it is a departmental assistant clerk and staff. After the control label being destroyed, the information department will log out of the data, use information management GUI, and upload it to the information management database.

(5) Change behavior: After replacing the mobile device, the employee submits the mobile device change application form to the information department. After receiving the application form, the information department uses the information management GUI to confirm whether the applicant is on the control list. After confirmation, the information management GUI is used to perform the procedures for data assault and label use. After the production being completed, the changed data are uploaded to the information management database.

(6) Procurement behavior: When the procurement staff needs to purchase information equipment, he/she submits the information equipment purchase application information to the information department. After receiving the application information, the department of information checks that the information equipment label, type, and manufacturer meet the requirements, and then forwards the application information to the accounting and statistics office. After the accounting and statistics office having submitted the application materials, it checks whether the name, amount, and application date of the application funds followed the regulations. After confirming that the application information followed the regulations, the accounting and statistics officers use the financial management GUI to make a posting and save it to the financial management database. After the storage being completed, the purchase check is issued to the purchasing personnel.

(7) Account creation behavior: The purchaser proposes a new procurement device and submits a request for establishing account to the logistics department. The logistics department will use the logistic GUI to apply for the state-owned property accounts and store the information in the logistics management database. After the logistics department adding the assets increase list, it will be sent to the information department. After receiving the property add-on form, the information department will create a new account using information management GUI and store the data in the information management database. After the data storage being completed, the information management GUI output control label is used and issued to the purchaser.

(8) Emergency response behavior: Barrack-area management staff fills in the status report form to the information department within 30 minutes after the incident. After receiving the status report form, the information department uses the information management GUI to confirm whether the information system in the barrack-area is invaded and uploads the status-utilization information management GUI to the information management database for reference. At the same time, the status report will be sent to the emergency response team. After the status report being completed, it is submitted the situation to the political warfare department. After the political warfare department receiving the information sheet from the information department, it will use the system to confirm the relevant laws and regulations. After the legal system having confirmed the law, the relevant law will be sent back to the Ministry of Political Warfare Department. After the political warfare department receiving the law and a press release being prepared, the situation was explained to the public in a
one-stop announce window. At the same time, the political warfare department will handle the situation alone to the public security office. After the public security office receiving the status statement from the political warfare department, the security protection mechanism was initiated and the employees in the barrack were safeguarded and supervised to ensure that no doubts were disclosed.

(9) Entry access control inspection behavior: The entry access control staff shall first require the personnel in and out of the barrack-area to show the mobile device. After confirming that the mobile device has completed the installation of the mobile MDM software and open it, its behavior was recorded by a mobile monitor or video recorder worn by the entry access control staff. After the end of the day, the video is sent to the department of information. The information department staff use the information management GUI to store it in the information management database for reference.

(10) Masking signal behavior: The mobile device signal barrier is set in the conference room. Before the meeting started, the barrack-area management staff opened the barrier and the mobile device frequency masker issued a signal to interfere with the employee’s mobile phone signal so that it would have no effect, thus achieving the purpose of prevention.

Table 1  
Description of Behaviors in AOISMMUMDC

| Behavior number | Behavior                          | External environment                                      | Component                                                                 |
|-----------------|-----------------------------------|----------------------------------------------------------|---------------------------------------------------------------------------|
| 1               | Application behavior              | Chief of information security officer, assistant clerk and staff | Information department, personnel department, personnel management GUI, personnel management database |
| 2               | Rewards and punishments behavior  | Information security officer, assistant clerk and staff   | Information department, information management GUI, document database      |
| 3               | Promulgated plan behavior         | Assistant clerk and staff                                 | Information department, personnel management GUI, information management GUI, information management database |
| 4               | Annullment behavior               | Assistant clerk and staff                                 | Information department, information management GUI, information management database |
| 5               | Change behavior                   | Assistant clerk and staff                                 | Information department, information management GUI, information management database |
| 6               | Procurement behavior              | Procurement staff                                         | Logistics department, logistics management GUI, information management GUI, information management database |
| 7               | Account creation behavior         | Procurement staff                                         | Logistics department, logistics management GUI, information management database |
| 8               | Emergency response behavior       | Barrack-area management staff, emergency response team, civilian, and assistant clerk and staff | Information department, information management GUI, information management database, political general department, legal affairs office, public security office |
| 9               | Masking signal behavior           | Entry access control staff                                | Mobile device MDM, mobile monitor, information department, information management GUI, information management database |
| 10              | Entry access control inspection behavior | Barrack-area management staff, assistant clerk and staff | Mobile device frequency masker |
Figure 6. Structure behavior coalescence diagram of AOISMMUMDC.
In Table 2, we can find out chief of information security officer, information security officer, emergency response team, civilian, entry access control staff have one behavior; barrack-area management staff has two behaviors; procurement staff have four behaviors. We can see the assistant clerk and staff initiated three interactive behaviors and ended with five behaviors in the SBC diagram of AOISMMUMDC, which means the assistant clerk and staff should be well-trained to fulfill the requirements and continuously improvement of information security management of using mobile device. Total of the external environment behaviors in ISSHCASIS are shown in Table 2.

| External environment | Total of interactive behaviors |
|----------------------|-------------------------------|
| Chief of Information Security Officer | 1 |
| Information security officer | 1 |
| Procurement staff | 4 |
| Assistant clerk and staff | 8 |
| Barrack-area management staff | 2 |
| Emergency response team | 1 |
| Civilian | 1 |
| Entry access control staff | 1 |

**Interaction Flow Diagram**

We apply interaction flow diagram (IFD) to demonstrate individual behavior. IFD is the sixth fundamental diagram that uses in achieving structure behavior coalescence. Each behavior presented on the SBCD of the AOISMMUMDC can be drawn as an IFD. The construction of IFD of the AOISMMUMDC describes the outside environment and structure elements, and their interactions according to the time. Each individual behavior is represented by an execution path. We use an IFD to define each one of these execution paths.

There are 10 interaction flow diagrams in total for the AOISMMUMDC: (1) interaction flow diagrams for application behavior of AOISMMUMDC; (2) interaction flow diagrams for rewards and punishments behavior of AOISMMUMDC; (3) interaction flow diagrams for promulgated plan behavior of AOISMMUMDC; (4) interaction flow diagrams for annulment behavior of AOISMMUMDC; (5) interaction flow diagrams for change behavior of AOISMMUMDC; (6) interaction flow diagrams for procurement behavior of AOISMMUMDC; (7) interaction flow diagrams for account creation behavior of AOISMMUMDC; (8) interaction flow diagrams for emergency response behavior of AOISMMUMDC; (9) interaction flow diagrams for masking signal behavior of AOISMMUMDC; and (10) interaction flow diagrams for entry access control inspection behavior of AOISMMUMDC.

Figure 7 represents IFD for entry access control inspection behavior of AOISMMUMDC. X-axis represents components and the external environment, in which information flow direction is from left to right. Y-axis represents the implementation of an interactive timeline from the top to the bottom in the time sequence. Figure 7 shows an IFD of the entry access control inspection behavior. First, actor entry access control staff interacts with the mobile device MDM component through the inspect entry access control operation call interaction, carrying no parameter. Next, component mobile device MDM interacts with mobile monitor component through the inspect record carrying no parameter. Next, mobile monitor component interacts with information management component through the checkup recorded video operation call interaction, carrying...
the recorded video input parameter. Continuously, information management component interacts with information management GUI component through the checkup recorded video operation call interaction, carrying the recorded video input parameter. Finally, information management GUI component interacts with the information management database component through the store recorded video operation call interaction, carrying the recorded video input parameter, as shown in Figure 7.

![Diagram](image)

*Figure 7. Interaction flow diagrams for entry access control inspection behavior of AOISMMUMDC.*

**Enterprise Interviews**

We interviewed with members of mobile device management related departments. We first described what constituted an architecture-oriented mobile device management approach and compared it with current process-oriented mobile device management practices to understand architecture-oriented mobile device management practices compared to process-oriented mobile devices. Was the management approach more appropriate? Members of this interview were all serving officers in the military. To protect their identities, the following titles are used on behalf of the staff. After discussions with two scholars and experts, the exhibition interview questions are as follows:

1. What is your opinion on the current information security management practices of the process-oriented mobile device?
2. Do you think that structure behavior coalescence approach is effective in making the organizational division of responsibility clearer?
3. After you being introduced to the architecture-oriented information security control practices of mobile devices in the barrack-area, what are your comments or suggestions on the architecture-oriented approach?
4. Do you have any problems or difficulties when using process-oriented mobile device management practices?
5. If your organization applies an architecture-oriented mobile device control practice, do you think there is a way to solve the problems that cannot be implemented with the control measures currently encountered?
(6) Do you think that the architecture-oriented information security control of mobile devices in the barracks will reduce the time required to handle the security incidents compared with the process guidance?

(7) Do you think that architecture-oriented information security control of mobile devices in the barracks will help you understand the use of resources in various organizations?

(8) Do you think that the architecture-oriented model will help increase the awareness of political employees about their own duties?

(9) Do you think architecture-oriented model can help you have a comprehensive understanding of the overall approach? If so, what are the reasons? If not, what are the reasons?

**Comparison Between Architecture-Oriented and Non-architecture-oriented Information Security Management Models for Using Mobile Device Control**

The architecture-oriented information security management for using mobile device control model is compared with the non-architecture-oriented model, and the results of the enterprise interviews are discussed.

**Comparison Between Architecture-Oriented and Non-architecture-oriented Information Security Management Model**

The architecture-oriented information security management model for using mobile device control is compared with the current process-oriented information security management model for using mobile device control practices. Through interviews with members of various departments in the military, we learn about the benefits and contributions of AOISMMUMDC to the current management operations using the SBC framework, as shown in Figure 8.

Non-architecture (process-oriented) security control model for mobile devices of personnel, often due to the relationship between the clauses leads to the delay of the operating time; and the architecture-oriented mobile device management and control practices, due to the information flow, the operation sequence, and the duration, can solve the imputation and the problems of division of human resources between departments and can effectively correct this problem. The current practice, which is presented in articles, is prone to deficiencies due to lack of clarity in the definition.

The six golden rules can help the mobile device to fully understand. The visual presentation is more understandable and more comprehensive than the article. The architecture-oriented mobile device control model enables clear division of human resources between logistics operations, enabling the employees to be aware of their own responsibilities, avoiding responsibilities, and reducing the waste of human resources. The architecture-oriented mobile device control practice can eliminate the management window period caused by unknown operation processes, as shown in Table 3.

**Analysis of Enterprise Interview Results**

On March 9th, 2018, we personally sent the interview questions to interviewee two weeks before the interviewing, and then set a schedule to Mr. S, the personnel manager of the personnel department; Ms. K, the section leader of the accounting and statistics office, Mr. B, the logistics manager of the logistics department; and Mr. C, commander of the guard of the department of entry access control and other mid- and high-level managerial personnel. After the interview, the verbatim version of the conversation record was completed and the respondent was asked to confirm it. After summarizing the interview contents, the following conclusions were drawn:
(1) Access control is part of the implementation level, so it is not easy to encounter regulatory issues. Entry access control staff believe that if the control method can be clearly defined, the access control can be implemented.

(2) In terms of personnel, it is often because of the relationship between the clauses that leads to delays in the operation time, and the architecture-oriented mobile device management and control methods can effectively solve the problems of imputation and inter-departmental services because of information flow, operation sequence and schedule, and correct the all problems.

(3) The diagrams of six golden rules help the mobile device to fully understand. The visual presentation is more understandable and more comprehensive than the articles.

(4) The architecture-oriented mobile device management and control model can clearly divide the logistics operations, make the employees aware of their own responsibility, avoid the occurrence of responsibilities, and reduce the waste of human resources.

(5) The architecture-oriented mobile device management control method can eliminate the management window period generated by unknown operation procedures.

(6) The lack of mobile device control needs to be improved. For example, the GPS positioning function in the MDM still needs to be strengthened. The iPhone can only be manually locked and the loopholes in the control can easily be created. The current practice is easy to present due to the clauses. Shirking the responsibility situations is still occurred.

(7) It is further recommended to make it easier to understand if you can animate the six golden rules. It is suggested that the concept of architecture-oriented can be used in the development of mobile device control system platform.

Table 3
Comparison Between Architecture-Oriented and Non-architecture-oriented Information Security Management Model for Using Mobile Device Control

| Items                              | Non-architecture-oriented information security management model for using mobile device control | Architecture-oriented information security management model for using mobile device control |
|------------------------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Architecture hierarchy            | Separation of structure and behavior makes structural hierarchy diagrams and behavioral hierarchy diagram independent of each other | Architecture hierarchy diagram makes complex companies easier to understand |
| Multiple view                      | Process-oriented Mobile device control model has enterprise behavioral view only and ignores other views | Architecture-oriented multiple view includes enterprise structural view, enterprise behavioral view, enterprise time view, enterprise analytical view, and enterprise designed view |
| Structure                          | Separation of structure and behavior                                                             | Structure behavior coalescence and enterprise structural view is the pillars of other views |
| Behavior                           | Separation of structure and behavior planned behavior                                           | Structure behavior coalescence and enterprise behavior is attached to the enterprise structure |
| Quality of mobile devices management and control | Solitary business processes cannot track the quality                                               | Enterprise architectural behavior can track the quality effectively |
| Department corporation and coordination | Solitary business processes have prevented departments from corporating and coordinating with each other | Enterprise architectural behavior can promote coordination and cooperation among various departments |
| Information integration            | Solitary business processes cannot integrate information from various departments             | Enterprise architectural behaviors have the effect of integrating all information |
| Departmental responsibilities      | Solitary enterprise processes cause all departments to care only about their own responsibilities | Architecture-oriented enterprise behavior can respect to others departmental responsibilities |
Figure 8. Comparison between architecture-oriented and non-architecture-oriented information security management model for using mobile device control.

Architecture-oriented information security management model for using mobile device control

Non-architecture-oriented information security management model for using mobile device control
Conclusions and Recommendations

This chapter will explain the research conclusions, research results, information security management implications, and future research proposed.

Conclusions

From the information security management and control of the military army, the management and control of mobile devices hardware and technology are not the key issues for improving the management. At present, there are many good mobile device management and control technology solutions that can be selected and can be achieved partially. The real problem effectiveness of management and control is how to integrate information security policies, mobile device management and control policies, executives’ responsibilities and implementation of management and control, and mobile device management and control of hardware and technology.

After comparing the fourth chapter architecture-oriented mobile device management model with the current practice, it is not difficult to find that although the Military Army has gradually opened mobile devices since 2014, its management methods, categories, and responsibilities have not been systematically sorted out. When it happens, it can only allow each department to make a difference. In the end, it can only cause a headache and give medical treatment. All departments are required to act according to their own operations within the department, not only cannot perform their duties, but also cause mutual restraint. This study makes a comprehensive review of the management methods of each department, establishes an architecture-oriented mobile device management model, and unifies the mobile device management and control model architecture.

However, this study also has its limitations: First, the respondents’ knowledge level is not consistent; the scope of employee covers graduates from high school to master’s degree; a considerable number of them have no information related background; and they have different levels of feelings about possible problems with mobile devices. Second, the scope of this research study is limited to a barrack-area, but not all Military Army; Third, although the National Security Command’s Safety and Security Notice No. A107003 expressly declares that in addition to the medical needs reported to the superior, mobile phone outside the mobile device all are not portable. However, there is no concrete method for the detection and prevention of mobile devices, which easily leads to a large loophole in information security protection.

Research Results and Information Security Management Implications

Mobile device information security has always been a dilemma for the military units. It is hoped that officers and soldiers can use new technology communication tools, but they also need to prevent the leakage of important military affairs and resources. This study has four implications on information security management of mobile device: (1) effective use of information security management resources: Once management resources cannot be effectively used, unwarranted waste will result from improper resource allocation, or management gaps may occur due to vacant control measures; (2) establishing the concept of mobile device information management: In the information security management of mobile devices, the information department must play a very important role. On many levels, the Ministry of Information of the military is required to work together with other departments to complete in the military unit, so the establishment of a comprehensive concept will contribute to information security management; (3) clear professional services of human resources control behavior: After the establishment of the general concept of the information security, it is necessary to clarify the professional services of human resources control and follow the business management and standard
operating procedures to perform their duties, mutual communication, and support to achieve the maximum synergy; and (4) strengthening the recognition of rights and responsibilities and information security: Finally, information security protection is not only the work of the information department, but also the consensus that all members of the organization should have. Therefore, in addition to trying to accomplish the tasks required by itself, it should understand the basic protection of information security, such as setting a strong password, access to the barrack-area need to start the mobile MDM, etc.; this kind of work should be done on their own cannot be ignored to achieve the goal of prevention information security events happened.

Recommendations

Due to differences in information security literacy among military personnel, visual architecture-oriented mobile device management models may not be universally accepted. It is suggested that scholars interested in this study will make the model animated explanation. Through animated explanation, the overall management approach will be explained in a simple and profound way, which can eliminate the gap between the information security knowledge and literacy of the people.

References

Chao, W. S., Chao W., & Chao H. (2008). System architecture: Software architecture, enterprise architecture, knowledge architecture, thinking architecture (1st ed.). Taipei: Science and Technology Books Co., Ltd. Publishing.

Chao, W. S. (2012). Systems architecture: SBC architecture at work. Taipei: LAP LAMBERT Academic Publishing.

Chao, W. S. (2013). Enterprise architecture: The cornerstone of business operation innovation. Taipei: Hao Sheng Culture and Education.

Chao, W. S. (2014). SBC view model. Retrieved March 30, 2018, from https://sites.google.com/site/sbcarchitecture/home/sbc-view-model

Chao, W. S. (2016). Systems architecture of smart healthcare cloud applications and services IoT system: General architectural theory at work. California, US: GreateSpace Independent Publishing Platform.

Gregg, M., Watkins, S., Mays, G., Ries, C., Bandes, R. M., & Franklin, B. (2006). Hack the stack. Burlington, MA: Syngress.

Hayes, D. R. (2014). A practical guide to computer forensics investigations. Hoboken, NJ: Pearson IT Certification.

ISO. (2015). ISO/IEC 27001:2013/Cor 2:2015, Information technology—Security techniques—Information security management systems—Requirements. Retrieved from https://www.iso.org/standard/54534.html

ISO. (2018). ISO/IEC 27000:2018, Information technology—Security techniques—Information security management systems. Retrieved April 30, 2018, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Ma, W. M. (2010). Study on architecture-oriented information security risk assessment model. In J. S. Pan, S. M. Chen, and N. T. Nguyen (Eds.), Computational collective intelligence: Technologies and applications (pp. 218-226). Berlin, Heidelberg: Springer.

Ma, W. M. (2014). Study on implement of the personal information protection act architecture for an university. International Conference on Business and Information (BAI 2014), July 3-5, Osaka, Japan.

Ma, W. M. (2016). A comparative study of information security management enterprise architecture-oriented model. BAI 2016, July 3-5, Kyoto, Japan.

Ma, W. M. (2017). Systems architecture of information security applications and services IoT system general architectural theory at work. BAI 2017, January 24-26, Winter, Bangkok, Thailand.