Extension of ISO/IEC27001 to Mobile Devices Security Management

Xiaobo Zhu and Yunqian Zhu(✉)

National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing, China
{zhu, zyq}@cert.org.cn

Abstract. Mobile security is more and more important with the fast growth of mobile devices, and people are becoming more dependent on mobile devices in their daily life. Malicious samples in mobile devices are growing in double times each year from 2011 to 2017 in China. ISO/IEC 27000 family of standards helps organizations keep information assets secure, such as financial information, intellectual property, employee details or information entrusted to you by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). However, ISO/IEC 27001 is not quite adaptable for mobile devices, because these developing mobile information devices lead to new challenges and security risks. This paper analyzes mobile devices security issues, and gives the drawback for 27001 in mobile security. Finally, this paper gives a consideration to these issues under ISO/IEC 27001 information security management system framework.

Keywords: Mobile security · Information security · ISO/IEC 27001 · ISMS

1 Introduction

Mobile devices are growing fast with more and more functions and good performance, such as laptops, personal digital assistants (PDAs) and handheld digital devices. Smartphones exceeded 55% of the mobile phone market [1]. Mobile devices are becoming a center of bank transaction, entertainment, communication, shopping and even work. However, mobile security is becoming more severe than ever, as shown in Fig. 1 [2]. These mobile devices provide significant value add to organizations but risks associated with their use need to be managed. Smart phones can be infected with malicious software, and sensitive data can be stolen. Phishing attacks work just as effectively with smartphones as with any other device.

Using a smart phone without security software has become unthinkable. With mobile phones, this sense of responsibility has not yet reached the majority of users, even though important personal data, personal photos and even company data can be stored on smartphones. Therefore, for an organization, mobile devices security management is much more important than ever before. ISO/IEC 27001 is the best-known standard providing requirements for an information security management system (ISMS).

X. Yun et al. (Eds.): CNCERT 2018, CCIS 970, pp. 27–35, 2019.
https://doi.org/10.1007/978-981-13-6621-5_3

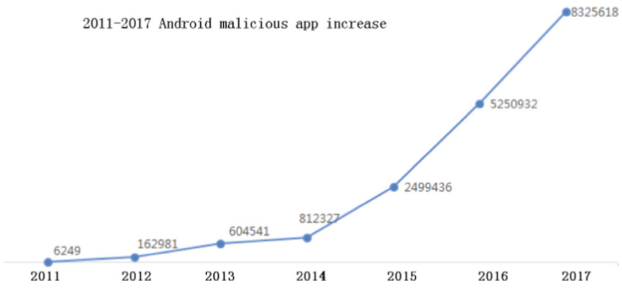

Fig. 1. 2011–2017 Android malicious app increase

2 ISO/IEC 27000 Family

2.1 Overview of ISO/IEC 27000 Family

ISO/IEC 27000 family of standards helps organizations keep information assets secure. Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS) [3]. Its new version is ISO/IEC 27000:2018. ISO/IEC 27000 family includes multiple standards for building Information Security Management System (ISMS), as show in Fig. 2.

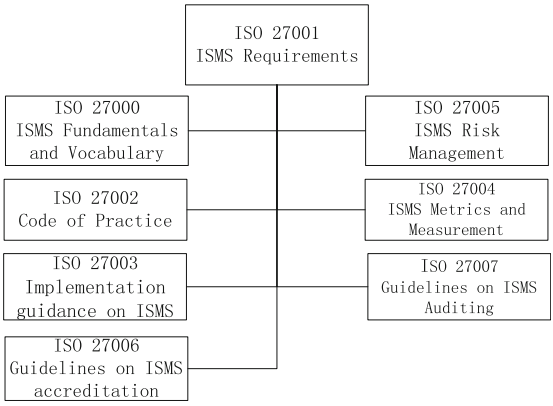

Fig. 2. ISO/IEC 27000 family

ISO/IEC 27001 is the only standard in this family that is used to providing certification for an organization. It outlines the ISMS framework by which an organization can build its own ISMS based on PDCA (Plan-Do-Check-Action) model. The other standards in this family provide profound support for an organization to build its own

ISMS. ISO/IEC 27002 provides choice from 133 concrete controls based on risk assessment. Though mobile devices covered, but it is not enough due to the ongoing technique limitations. ISO/IEC 27003 is ISMS Implementation guidance which implements PDCA in more detail, including identification of assets, threat identification, risk assessment, analysis and improvement of controls. ISO/IEC 27004 is ISMS Metrics and measurement which evaluates effectiveness of information security controls and objectives. ISO/IEC 27005 is ISMS Risk Management which is a new standard that is mainly concerned with risks. ISO/IEC 27006 is Guidelines on ISMS accreditation. ISO/IEC 27007 is Guidelines on ISMS Auditing.

2.2 Plan-Do-Check-Action Process

According to 27001, ISMS is built via a 4-phase process called PDCA (Plan-Do-Check-Action) process, as shown in Fig. 3. In each phase, there are different activities. In phase PLAN, there is only one activity called "establish ISMS". In phase DO, there exist two activities, called "Implement and operate the ISMS". In phase CHECK, there are two activities called "monitor and review ISMS". In ACT phase, two activities called "maintain and improve" are involved.

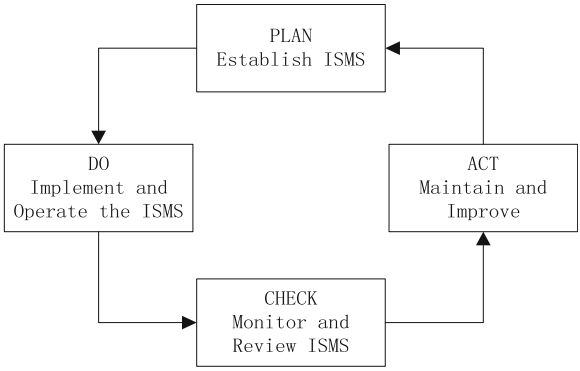

Fig. 3. PDCA process.

2.3 ISO/IEC 27001 Summary

ISO/IEC 27001:2013 provides 14 control domains (2005 version is 11) and 113(2005 version is 133) controls for information security. The ISO/IEC 27001 categories are shown in Fig. 4. The form is as shown in Fig. 5.

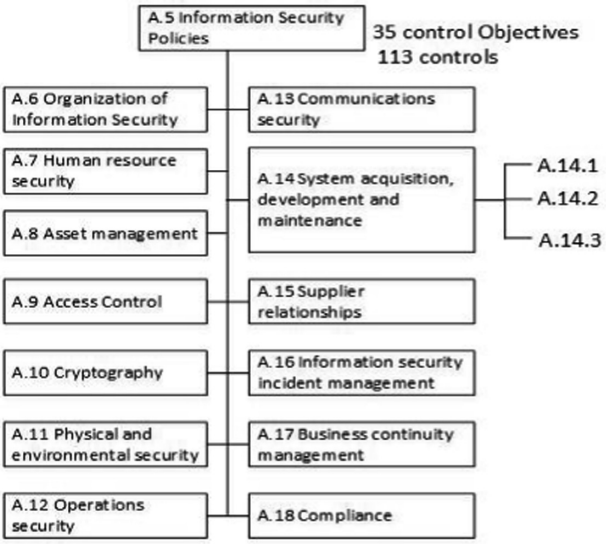

Fig. 4. ISO/IEC 27001 categories.

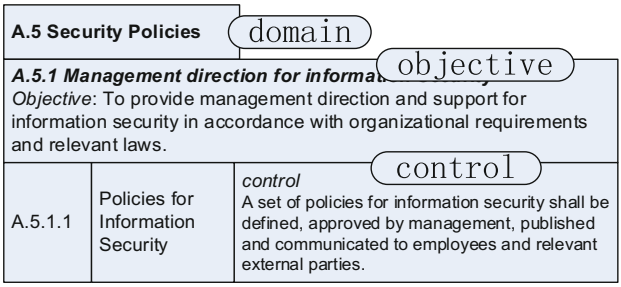

Fig. 5. Form of ISO/IEC 27001 domain, objective and control.

However, these control objectives and controls are mostly too general, and for mobile devices information security it is not quite adaptable.

3 Analysis of Mobile Devices Security Management

Mobile Devices are widely used in any organization, and also the mobile device security management is every important. Therefore, issues and risks of mobile devices security management must be recognized. Due to the rapid development of mobile device technique, numerous new problems arise from the absence of management to the specific consideration of mobile devices.

3.1 Easy Information Disclosure via Mobile Devices

Even though a strict security system has been built in accordance with ISO/IEC 27001, and firewalls or IDS/IPS is deployed in an organization. However the organization is still in great risk under the circumstances of mobile services. For example, a user can photo the screen with a smartphone when dealing with something important, and then the important content displayed in screen is already in the Internet if the mobile phone is in the Internet. Information disclosure is quite simple and easy with mobile devices. It is not proper for an organization to force its staff no to use mobile devices. Meantime, mobile devices are easily controlled by unauthorized access due to the users low security awareness, so mobile devices will bring high risk if they are controlled by malicious app.

3.2 High Computing Ability of Mobile Devices

Many mobile devices such as smartphones or PDAs are now equipped with fast processor and embedded operating system (OS). Many applications specific to embedded OS are developed and deployed. As a matter of fact, such mobile devices are powerful computers. Meantime, these devices are usually installed with multiple communication measures, such as Bluetooth, TCP/IP protocols, etc.

With these rich and powerful features, vulnerabilities are also exposed to potential adversary, who can exploit these vulnerabilities to attack mobile devices. Therefore, the mobile devices have become a prized target, where there are increased numbers of malware targeted at intercepting valuable data [5].

3.3 Vague Security Border

End-to-end information assets always have limited and controlled boundary. For example, a PC or server will always be placed somewhere of a building, and so the security border can be easily recognized and controlled. But with mobile devices, it is hard to control the range or border of mobile devices. So, the security boundary is becoming vague under the existence of mobile devices. It seems in anywhere.

3.4 Versatile Function of Mobile Devices

USB drives can now store much more software, and so it is quite easy to make a USB drive as a booting disk which can easily go into a PC disks but avoid the protection software of that PC. A smart phone can have 128 G storage space with versatile functions such as recording, photograph, GPS, etc. Therefore, mobile devices can play more functions, such as storing data, booting system, mp3 player, etc. It is convenient for people to use mobile devices, but it is in high risk when using these versatile functions of mobile devices.

3.5 Cross-border Information Theft

Mobile devices can be anywhere, as the inherent mobility (beginning from laptops) has always made it impossible to rely on a strong perimeter for adequate protection. The cloud computing revolution and the myriad of hosted application services that are not geographically fixed has made it easier for data to cross national borders [6]. With the increased use of mobile network, the applications and data stored in mobile devices lost locally and globally, may put critical infrastructure at risk. In addition, data travelling on the mobile devices is typically subject to laws and regulations that will vary from one jurisdiction to another.

3.6 Data Disposal

The amount of data that can be stored and processed in mobile devices has been growing dramatically. Inappropriate device disposal procedures may bring the risk of sensitive information being retained on the device and unauthorized access. Organizational computing assets should be subject to company asset management procedures which should include secure disposal for assets containing sensitive data. However, the execution of these procedures can often be a grey area when dealing with personal devices in the workplace. This requires clear organizational policies in order to safeguard sensitive, confidential and highly valued information (including commercial intelligence).

4 Mobile Devices Security Under ISO/IEC 27001 Framework

4.1 Information Security Policy Consideration

As ISO/IEC 27001 says, the objective of information security policy is to set up management direction and support for information security. Information Security Policy is a directive and strategic file which includes the goal and strategy of information security. As the mobile devices security is particularly important and weak, so it must be particularly shown and considered in Information Security Policy and Information Security Policy should include the following aspects: information security view, objective, strategy, range, organizational structure, responsibility, assets, etc. Especially, policy relating to mobile devices should be effective, definite and complete. However, concrete and detail process should not covered in policy.

Developing information security policy should obey to a flow: (1) determine the range of information security policy, (2) assess and analyze risk, and (3) check, approve and implement information security policy. While developing information security policy, advanced information security technique on mobile devices is the basic assurance. All related techniques should be collected and updated in time.

4.2 Organization of Information Security

Information security will be managed within an organization. Management will approve information security policies, assign security roles, and coordinate and review the implementation of security across the organization. Information assets and information technology regarding to mobile devices must be recognized and updated in time.

4.3 Human Resources Security

Mobile devices are always used by people, so human resources security is important. Everyone in an organization must understand his or her responsibilities and will know the manners to reduce the risk of theft, fraud or misuse of mobile devices. Thus, responsibilities should be divided into different layers. The top layer usually monitors and audits the information security activities of an organization. The second layer manages the routine information security activities. The third layer is mobile device owner who operates mobile devices according the policy, and is subject to upper layer's management.

4.4 Physical and Environmental Security

Though mobile devices have not limited boundary, physical and environmental security must be considered in order to prevent unauthorized physical access, damage, theft, compromise, and interference to mobile information and facilities. Locations housing mobile devices will be secured with appropriate security barriers and entry controls. They will be physically protected from unauthorized access, damage and interference. Secure areas will be protected by appropriate security entry controls to ensure that only authorized personnel are allowed access. Security will be applied to off-site equipment. All equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal in compliance with statewide policies.

4.5 Communications and Operations Management

There are much more communications and operations for mobile devices than for other devices. Responsibilities and procedures for administrating mobile devices must be established according to information security policy. Virus and malicious code for mobile devices should be detected protect the integrity of software and information in mobile devices. Exchange of sensitive data with other organizations must be done based on a formal exchange policy. Mobile devices containing sensitive data will be protected against unauthorized access, misuse.

4.6 Access Control

For an organization with mobile devices, access control includes two aspects: one is access to organizational information systems from mobile devices, the other is access to outer information facilities from mobile devices. Both these two aspects of access control for mobile devices should be controlled on the basis of business and security requirements. Formal procedures should be established for the mobile devices to control access rights to both inner and outer information facilities, to prevent unauthorized access.

5 Conclusion

Extension of ISO/IEC 27001 Information security management with mobile devices always meets new challenges with the rapid development of mobile technique. This paper analyses the issues of information security with mobile devices. It is a good practice with ISO/IEC 27000 information security series standards. The design, operation, use, and management of mobile information assets are subject to statutory, regulatory, and contractual security requirements in order to avoid breaches of any law.

The following controls are a good reference for Information Security Management system under ISO/IEC 27001 framework.

- Never set the login dialog box to remember the password;
- Keep antivirus protection up-to-date, as well as the operating system and application security patches;
- Password-protect all devices, such as removable drives and compact disks (CDs);
- Do not store unencrypted sensitive information on mobile devices;
- Incorporate a time-out function that requires re-authentication after 30 min of inactivity;
- Back up your data to a location separately from the device;
- Include both hardware/device-based authorization and application-based authorization for access control mechanisms;
- Do not keep mobile devices online when not in use. Either shut them off or physically disconnect them from the Internet connection;
- Lost or misplaced government-issued devices must be immediately reported to management.

References

1. Conti, M.: Body, Personal and local ad hoc wireless networks. In: Ilyas, M. (ed.) The Handbook of Ad Hoc Wireless Networks. CRC Press LLC, Boca Raton (2003)
2. http://www.aqniu.com/industry/32319.html
3. https://www.iso.org/isoiec-27001-information-security.html
4. http://www.comscore.com/ger/Insights/Presentations_and_Whitepapers/2013/The_Mobile_Shift

5. Kao, I.: Securing Mobile Devices in The Business Environment. IBM Global Technology Services – Thought Leadership White Paper, October 2011
6. Ernst & Young: Data Loss Prevention: Keeping Your Sensitive Data Out of The Public Domain, Insights on IT Risk Business Briefing (2012)
7. ISO/IEC 27000:2009: Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary. ISO/IEC, Geneva (2009)
8. ISO/IEC 27001:2005: Information Technology—Security Techniques—Information Security Management Systems—Requirements. ISO/IEC, Geneva (2005)
9. ISO/IEC 27002:2005: Information Technology—Security Techniques—Information Security Management Systems—Code of Practice for Information Security Management. ISO/IEC, Geneva (2005)
10. ISO/IEC 27003:2010: Information Technology—Security Techniques—Information Security Management System Implementation Guidance. ISO/IEC, Geneva (2010)
11. ISO/IEC 27004:2009: Information Technology—Security Techniques—Information Security Management—Measurement. ISO/IEC, Geneva (2009)
12. ISO/IEC 27005:2008: Information Technology—Security Techniques—Information Security Risk Management. ISO/IEC, Geneva (2008)