Auditing Mobile Devices

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2gimJq5

By the time this article is published, it will have been about 20 months since the US Federal Bureau of Investigation (FBI) unlocked the iPhone of the San Bernardino, California, gunman who killed 14 people.[1] The request by the FBI for Apple to build new software to unlock the mobile device resulted in strongly held opinions on encryption and backdoors on both sides[2] that have yet to be resolved. I have sympathy for all involved, but, as a technologist, I passionately believe that backdoors should not be developed. This conviction has been strengthened by the recent WannaCry[3] and Petya[4] attacks, which were developed using the leaked Shadow Brokers exploit, EternalBlue, which is generally believed to have been developed by the US National Security Agency (NSA).

Although a critical issue, this is not the focus of this column, nor is it something that we, as IT auditors, can influence on a day-to-day basis. However, an aspect of this case that received little or no coverage was the fact that San Bernardino County owned mobile device management (MDM) software that was not installed on the device.[5] This would have allowed its IT department to remotely unlock the phone and, in my opinion, save the reputation of the organization in question. This is a risk that IT auditors can and should influence. So how can practitioners audit to help mitigate this and other mobile device risk scenarios?

In a previous column,[6] I advocated the use of an ISACA® paper on creating audit programs.[7] This process can be applied to build an audit program for mobile devices for an organization.

Determine Audit Subject

The first thing to establish is the audit subject. What does a mobile device mean in the enterprise? If there are distinct types of mobiles devices in use, they should probably be recorded as separate audit universe items. ISACA categorized mobile devices (**figure 1**) in a 2012 white paper[8] while an earlier white paper[9] listed the type of mobile devices:

- Full-featured mobile phones with personal computer-like functionality, or smartphones
- Laptops and netbooks
- Tablet computers
- Portable digital assistants (PDAs)
- Portable Universal Serial Bus (USB) devices for storage (such as thumb drives and MP3 devices)
- Connectivity (such as Wi-Fi, Bluetooth and HSDPA/UMTS/EDGE/GPRS modem cards)
- Digital cameras
- Radio frequency identification (RFID) and mobile RFID (M-RFID) devices for data storage, identification and asset management
- Infrared-enabled (IrDA) devices such as printers and smart cards

In 2017, wearables, including smart watches, can certainly be added to that list. The key is to use the guidance to consider mobile devices in use at an enterprise and determine the audit subject(s). One needs to answer the key question: What is being audited?

Ian Cooke, CISA, CGEIT, CRISC, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt
Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has 30 years of experience in all aspects of information systems. Cooke has served on several ISACA committees and is a current member of ISACA's CGEIT® Exam Item Development Working Group. He is the community leader for the Oracle Databases, SQL Server Databases, and Audit Tools and Techniques discussions in the ISACA Knowledge Center. Cooke supported the update of the *CISA Review Manual* for the 2016 job practices and was a subject matter expert for ISACA's CISA and CRISC Online Review Courses. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules. He welcomes comments or suggestions for articles via email (Ian_J_Cooke@hotmail.com), Twitter (@COOKEI), or on the Audit Tools and Techniques topic in the ISACA Knowledge Center. Opinions expressed are his own and do not necessarily represent the views of An Post.

Define Audit Objective

Once what is being audited has been determined, the objective of the audit needs to be established. Why is it being audited? From an auditor's perspective, it is advisable to adopt a risk-based view and define the objectives accordingly.[10]

- Identify the risk associated with the devices (**figure 2**).

Figure 1—Mobile Device Categories

Category	Devices	Examples
1	Data storage (limited), basic telephony and messaging services, proprietary operating system (OS) (limited), no data processing capability	• Traditional cell phones
2	Data storage (including external) and data processing capabilities, standardized OS (configurable), extended services	• Smartphones • Early pocket PC devices
3	Data storage, processing and transmission capabilities via alternative channels, broadband Internet connectivity, standardized OS (configurable), PC-like capabilities	• Advanced smartphones • Tablet PCs

Source: ISACA, *Securing Mobile Devices*, USA, 2012

Figure 2—Mobile Device Vulnerabilities, Threats and Risk

Vulnerability	Threat	Risk
Information travels across wireless networks, which are often less secure than wired networks.	Malicious outsiders can do harm to the enterprise.	Information interception resulting in a breach of sensitive data, damage to enterprise reputation, nonadherence to regulation, legal action
Mobility provides users with the opportunity to leave enterprise boundaries and, thereby, eliminates many security controls.	Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this malware into the enterprise network.	Malware propagation, which may result in data leakage, data corruption and unavailability of necessary data
Bluetooth technology is convenient for many users to have hands-free conversations; however, it is often left on and then is discoverable.	Hackers can discover the device and launch an attack.	Device corruption, lost data, call interception, possible exposure of sensitive information
Unencrypted information is stored on the device.	In the event that a malicious outsider intercepts data in transit or steals a device, or if the employee loses the device, the data are readable and usable.	Exposure of sensitive data, resulting in damage to the enterprise, customers or employees
Lost data may affect employee productivity.	Mobile devices may be lost or stolen due to their portability. Data on these devices are not always backed up.	Workers dependent on mobile devices unable to work in the event of broken, lost or stolen devices and data that are not backed up
The device has no authentication requirements applied.	In the event that the device is lost or stolen, outsiders can access the device and all of its data.	Data exposure, resulting in damage to the enterprise and liability and regulation issues
The enterprise is not managing the device.	If no mobile device strategy exists, employees may choose to bring in their own, unsecured devices. While these devices may not connect to the virtual private network (VPN), they may interact with email or store sensitive documents.	Data leakage, malware propagation, unknown data loss in the case of device loss or theft
The device allows for installation of unsigned third-party applications.	Applications may carry malware that propagates Trojans or viruses; the applications may also transform the device into a gateway for malicious outsiders to enter the enterprise network.	Malware propagation, data leakage, intrusion on the enterprise network

Source: ISACA, *Securing Mobile Devices*, USA, 2012

- Define objectives for each category or type of selected device; refer to information value and information risk. This is key.
- Focus on a limited number of audit objectives for a reasonable scope.

It is worth noting that although ISACA's *Securing Mobile Devices* white paper considered the vulnerability of the enterprise not managing the device, it did not consider a San Bernardino County scenario. The lesson? Spend some time considering emerging risk scenarios.

Audit objectives should also correspond to security and protection goals as defined by the enterprise (**figure 3**).[11]

Set Audit Scope

When the objectives of the audit have been defined, the scoping process should identify the actual mobile devices that need to be audited. In other words, what are the limits to the audit? This could include devices in a specific country, region or division; devices that are used for a specific purpose; or devices that contain especially sensitive data. Again, this should be risk based. Also, consider if personally owned devices (bring your own device [BYOD]) should be included.

> **"When the objectives of the audit have been defined, the scoping process should identify the actual mobile devices that need to be audited."**

Perform Pre-Audit Planning

Now that the risk has been identified (**figure 2**), it should be evaluated to determine its significance.

Figure 3—Organizational Security Goals and Audit Objectives

Security Goal	Audit Objective
Mobile device security policies and procedures are adequate and effective.	Obtain assurance over mobile device security policies and related controls at the entity level, general level and detailed control level.
Access control and encryption for mobile devices are adequate and comprehensive.	Review mobile device access controls and encryption controls in line with data and information risk as well as information classification.
Data and information segregation in brought-in devices is complete and effective.	Review concepts, methods and implementation of data and information segregation for all devices owned by and brought in by end users.
Mobile device security incident management is fully implemented and effective.	Review mobile device incident management processes and controls, and obtain assurance over the effective functioning of incident management.

Source: ISACA, *Securing Mobile Devices*, USA, 2012

Conducting a risk assessment is critical in setting the final scope of a risk-based audit.[12] The more significant the risk, the greater the need for assurance. Assurance considerations for mobile devices include:[13]

- **Policy**—Does a security policy exist for mobile devices? Does it include rules for appropriate physical and logical handling? The enterprise should have a policy addressing mobile device use and specifying the type of information and kinds of devices and information services that may be accessible through the devices.
- **Antivirus updates**—Auditors should verify that the enterprise updates the mobile device antivirus software to prevent perpetuation of malware.
- **Encryption**—Auditors should verify that any data labeled as sensitive are properly secured while in transit or at rest.
- **Secure transmission**—Auditors should determine whether mobile device users are connecting to the enterprise network via a secure connection. VPN, IP Security (IPsec) or Secure Sockets Layer (SSL) can offer some levels of assurance.
- **Device management**—Auditors should determine whether there is an asset management process in place for tracking mobile devices. This asset management program should also detail procedures for lost and stolen devices as well as procedures for employees who have been terminated or have resigned from the enterprise.
- **Access control**—Auditors should verify that data synchronization of mobile devices is not set to receive access to shared files or network drives that contain data that are prohibited for mobile use by the policy.
- **Awareness training**—The auditor should verify that the enterprise has an awareness program in place that addresses the importance of securing the mobile devices physically and logically. The training should also make clear the types of information that can and cannot be stored on such devices.
- **Risk**—Mobile devices have the capability to store large amounts of data and present a high risk of data leakage and loss. As such, mobile device policies should be created and enforced to ensure that information assets are not exposed.

The use of any mobile device encompasses several legal relationships and obligations that must be considered when auditing or reviewing devices. In partial or full BYOD scenarios, further legal obligations may arise from the fact that parts of the mobile device (and information) are considered beyond the control of the enterprise.[14] Furthermore, when the device is used for private purposes—even to a very small extent—questions of personal data protection and privacy will inevitably arise. In most jurisdictions, privacy is protected by law and additional regulations.[15] If any doubt exists, it is prudent to seek legal advice in the relevant jurisdiction.

> **“Audit programs should be considered a starting point and adjusted based upon risk and criteria that are relevant to the organization that is being audited.”**

Finally, the auditee should be interviewed to inquire about activities or areas of concern that should be included in the scope of the engagement. Once the subject, objective and scope are defined, the audit team can identify the resources needed to perform the audit work.[16]

Determine Audit Procedures and Steps for Data Gathering

At this stage of the audit process, the audit team should have enough information to identify and select the audit approach or strategy and start developing the audit program.[17] There is enough information to decide what documents are expected to be seen, what laws and regulations apply, the criteria and whom the audit team is going to interview. However, the testing steps do need to be defined.

In August 2017, ISACA released an updated version of its *Mobile CoÜuting Audit/Assurance Program,*[18] which defines testing steps for mobile devices. Some readers may have just thought, “Why did he

Enjoying this article?

- Read *Mobile Computing Audit/ Assurance Program.* *www.isaca.org/auditprograms*
- Learn more about, discuss and collaborate on mobile computing in the Knowledge Center. *www.isaca.org/mobile-computing*

not just state this at the beginning of the article?" I refer those readers back to this author's first column.[19] Audit programs should be considered a starting point and adjusted based upon risk and criteria that are relevant to the organization that is being audited. Failure to do so can result in a checklist approach, which can lead to the auditor recommending controls that are not applicable to the organization. This, in turn, can damage the auditor's reputation with the auditee and, ultimately, with senior management.[20] It is worth spending the time considering the risk and the resulting need for assurance (**figure 4**).

Figure 4—Assurance Consideration to Audit Program Mapping

Assurance Consideration	Audit Program Process Sub-Area
Policy	Mobile computing policy
Antivirus updates	Anti-malware protection
Encryption	Device protections
Secure transmission	Wireless access points
Device management	Removable media/remote storage solutions/data recovery/asset management
Access control	Secure access/identification and authentication
Awareness training	User training
Risk	Risk management

Key testing steps in the audit program include password controls and the configuration of the selected MDM solution (if one is in place). Excellent guidance is provided on these and other aspects of mobility by the US Department of Defense (DoD) information systems Security Technical Implementation Guides (STIGs).[21]

Conclusion

As the uses, storage capabilities, power and proliferation of mobile devices have increased, so has the risk they pose to an enterprise. As a leading advocate for managing this risk, ISACA has produced several white papers in this area. Each of these documents is worth consulting to develop an audit/assurance program that is tailored to the individual enterprise. Failure to do so can result in a checklist approach, which can lead to a failure to mitigate key and emerging risk.

"As the uses, storage capabilities, power and proliferation of mobile devices have increased, so has the risk they pose to an enterprise."

Endnotes

1 Burgess, M.; "FBI Unlocks Shooter's iPhone Without Apple's Help," *Wired*, 29 March 2016, *www.wired.co.uk/article/apple-fbi-unlock-iphone-5c-court-order-dropped*

2 Elmer-DeWitt, P.; "Apple vs. FBI: What the Polls Are Saying—Updated," *Fortune*, 23 February 2016, *http://fortune.com/2016/02/23/apple-fbi-poll-pew/*

3 Symantec Security Response, "What You Need to Know About the WannaCry Ransomware," 12 May 2017, *https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware*

4 Symantec Security Response, "Petya Ransomware Outbreak: Here's What You Need to Know," 27 June 2017, *https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know*

5 Finkel, J.; "Exclusive: Common Mobile Software Could Have Opened San Bernardino Shooter's iPhone," Reuters, 19 February 2016, *www.reuters.com/article/us-apple-encryption-software-exclusive-idUSKCN0VS2QK*

6 Cooke, I.; "Audit Programs," *ISACA® Journal*, vol. 4, 2017, *www.isaca.org/Journal/archives/Pages/default.aspx*
7 ISACA, "Information Systems Auditing: Tools and Techniques, Creating Audit Programs," USA, 2016, *www.isaca.org/Knowledge-Center/Research/Documents/IS-auditing-creating-audit-prograÙ_whp_eng_0316.PDF*
8 ISACA, *Securing Mobile Devices*, USA, 2012, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices-Using-COBIT-5-for-Information-Security.aspx*
9 ISACA, *Securing Mobile Devices*, USA, 2010, *www.isaca.org/Knowledge-Center/Research/Documents/SecureMobileDevices_whp_Eng_0710.pdf*
10 *Op cit*, ISACA, 2012, p. 89
11 *Ibid*.
12 ISACA, *Audit Plan Activities: Step-By-Step*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/Documents/Audit-Plan-Activities_res_eng_0316.pdf*
13 *Op cit,* ISACA, 2010, p. 9
14 *Ibid*., p. 91
15 *Ibid*., p. 94
16 *Op cit,* ISACA, 2016
17 *Ibid*.
18 ISACA, *Mobile CoÜuting Audit/Assurance Program*, USA, 2017, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Mobile-CoÜuting-Audit-Assurance-Program.aspx*
19 *Op cit,* Cooke
20 *Ibid*.
21 Department of Defense, Security Technical Implementation Guides (STIGs), USA, *http://iase.disa.mil/stigs/mobility/Pages/index.aspx*