book review

Securing Mobile Devices

Reviewed by Larry Marks, CISA, CISM, CGEIT, CRISC, CFE, CISSP, CSTE, ITIL, PMP, who is a risk manager with extensive experience in managing and implementing processes, policies and technology regarding risk, security, governance, program management, compliance, internal controls and information security in financial services, insurance, health care and telecommunications industries. He has helped manage project management offices at various Fortune 100 firms. Marks has been published in the *ISACA Journal*, *the (ISC)² Journal*, the *PMI Journal* and *ProjectManagement.com*.

Securing Mobile Devices is a short book from ISACA's Cybersecurity Nexus intended to guide security professionals and governance, risk and compliance personnel in how to use the COBIT® 5 framework to obtain assurance in auditing and reviewing mobile devices. This book defines mobile devices as laptops, personal digital assistants (PDAs), cell phones, headsets and tablets.

The authors then expand the concept of mobile by indicating that the controls can apply to the Internet of Things (IoT). IoT is defined by the authors to include medical implants, wearable computing devices or automobiles connected to the cellular network. The authors take a forward-thinking approach by providing a framework for managing security for mobile devices. The book covers the people, process, technology, principles, skills, infrastructure and applications that security professionals need to ensure the control posture of devices. It also provides information on security configuration guidelines when performing a forensic review.

While the controls and guiding principles in the book do not cover patching mobile devices, tying the devices into the overall end-point security program for the enterprise, monitoring of user activity on the devices, or the impact of the IoT on these controls, they do map well to COBIT 5 and enable the reader to have an understanding of how the controls relate to mobile devices. The book does not cover penetration testing or red-blue testing of the mobile security network.

Securing Mobile Devices emphasizes the importance of collaboration among business, IT, security, legal and compliance to ensure that controls are properly designed and implemented. A strong and well-thought-out framework is required to ensure success, and this book helps enterprises better utilize COBIT® for that purpose. It is also useful to reference an article titled, "Mobile App Security Audit Framework," which appeared in volume 4, 2016, of the *ISACA® Journal*, which can serve as a helpful supplement to this book. Although the article's author stripped away all other mobile devices such as laptops and IoT and concentrated on mobile security devices, he came to the same conclusions as the authors of this book: the benefits of collaboration and the need for a strong framework. Leveraging both the book and the article is likely to aid in understanding and evaluating the risk in operating with mobile devices in an organizational environment.

Despite being written in 2011 and published in 2012, this book is well mapped to *COBIT® 5 for Information Security*. Security professionals can reference this book for the principles that can help ensure mobile security. Additional guidance is needed for the security professional who intends to audit IoT to help him/her with reviewing the impact of IoT on these controls and identifying the compensating controls, gaps and areas where a risk exception may be required; this may be a fruitful area for a future publication.

Editor's Note

Securing Mobile Devices is available from the ISACA® Bookstore. For information, visit *www.isaca.org/bookstore*, contact support at *https://support.isaca.org/* or telephone +1.847.660.5650.