Commercial Mobile Devices and Organizational Cyber Security

Christopher Furton

Syracuse University

Commercial Mobile Devices and Organizational Cyber Security

Commercial Mobile Devices are critical to organizations and, if implemented and used properly, are a business-enabler that significantly enhances communication. For the purpose of this paper, Commercial Mobile Device (CMD) is defined as any portable device that is purchased from a commercial vendor that processes, stores, and/or transmits organizational information. Laptops, smart phones, external media such as flash media or external hard drives, and digital cameras are all common examples of CMDs in use throughout many organizations. Although these devices provide flexibility and mobility to businesses, considerations must be made to secure what is stored on devices, how the device communicates back to the organization, and how users authenticate to the device. Additionally, the policy aspects must also be considered.

Many of today's devices have the ability to store user information. That stored information, often referred to as Data at Rest (DAR), needs to be safeguarded to prevent unauthorized access. If lost or stolen, the contents of the mobile device are encrypted preventing compromise of the information. Several commercial off the shelf programs are available to provide DAR encryption for laptops and external media. Additionally, some manufacturers, Blackberry for example, offer built in DAR using Content Protection functionality (Research in Motion Ltd). Although DAR encyption protects the confidentiality of the information contained, potential impacts to availability exist as encrpyted data requires key management to decrpyt and, if not done properly, may result in information that can not be accessed by the user (EMC Corporation, 2008).

In addition to data at rest, data needs to be secured while it is in transit to and from the organization. Data in Transit (DIT) can be protected at the protocol level using secure web browsing, secure file transfer, or secure shell (Vesperman, 2002) or by using encrpytion techniques for all the traffic at once. Virtual Private Networks (VPN) is a common mechanism for providing DIT encryption. When a mobile device uses VPN, all traffic is encrypted and sent back to the organization making a logical secure pipe between organization and device. VPN technology can also leverage the organization's access control system so that users remotely authenticate to the organizations network even though the computer is not physically connected (Cisco, pg 2).

As VPN technology can utilize the organizations access controls, other technologies exist to prevent unauthorized users from accessing mobile devices. Two-factor authentication can provide the needed access control security by requiring the user to present a token (something you have) and a password or pin (something you know) before gaining access to the device. The token can be a smartcard with a reader or use transient authentication built into everyday wearable items such as the IBM Linux wristwatch (Sun, Huai, Sun, Zhang, & Feng, 2008). Other access control technologies like biometrics are able to identify the user using biological or behavior traits like fingerprints or speech (Kim, Chung, & Hong, 2010).

Regardless of which access control technology is used, it is important to regulate access to mobile devices and ensure policy is in place to support those technologies. Policy should be written that explains acceptible use for mobile devices and which devices are allowed. For example, policy should prevent usage of personally owned devices and discuss what level the organization's devices can be used with other personal equipment. Allowing users to use portable storage devices between organizational computers and home computers poses a risk that can be mitigated by providing anti-virus for home use. Additionally, the policy should dictate restrictions on information classification that can be stored on portable devices. For example, storing information that is privacy sensitive or business propriatary is prohibited. The details for proper use should be outlined in policy and strictly enforced.

In conclusion, with the proper technical and policy measures in place, using mobile devices within an organization can provide value. By ensuring the data is encrypted on the device, between the device and the organization, and ensuring that the devices have proper access controls, some of the risk associated with using removable devices can be mitigated. Lastly, the organization should have the proper policy to outline acceptible use. Organizations should embrace todays mobile devices and implement the needed measures to protect their infrastructure.

Bibliography

Cisco. (n.d.). *Cisco Secure Remote Access—Cisco ASA 5500 Series SSL/IPsec.* Retrieved June 24, 2011, from Cisco Data Sheet: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd80402e3f.pdf

EMC Corporation. (2008). *Approaches for Encryption of Data-at-Rest in the Enterprise, A Detailed Review.* Hopkinton, MA: EMC Corporation.

Kim, D.-J., Chung, K.-W., & Hong, K.-S. (2010, November). Person Authentication using Face, Teeth, and Voice Modalities for Mobile Device Security. *IEEE Transactions on Consumer Electronics, 56*(4), 2678-2685.

Research in Motion Ltd. (n.d.). *Blackberry Help Center*. Retrieved June 22, 2011, from Manuals for Blackberry Users: http://docs.blackberry.com/en/smartphone_users/deliverables/1487/About_content_protection_29009_11.jsp

Sun, D.-Z., Huai, J.-P., Sun, J.-Z., Zhang, J.-W., & Feng, Z.-Y. (2008, November). A New Design of Wearable Token System for Mobile Device Security. *IEEE Transaction on Consumer Electronics, 54*(4), 1784-1789.

Vesperman, J. (2002). *Introduction to Securing Data in Transit.* Open Content.

About the author

Author: Christopher Furton

Website: Http://christopher.furton.net

Certified professional with over 12 years of Information Technology experience and 8 years of hands-on leadership. An expert in cyber security with both managerial and technical skills proven throughout a career with increasing responsibility and performance expectations. Known ability to translate complex information for universal understanding. Detail-driven, results-focused leader with superior analytical, multitasking, and communication skills. Well-versed in industry best practices including Project Management and IT Service Management. Currently holding active CISSP, CEH, ITIL Foundations, Security+, and Network+ certifications.

Visit the auhor’s blog:
IT Management Perspectives - https://christopherfurton.wordpress.com/

Social Sphere:

LinkedIn	Twitter	Google+	Quora	Wordpress	Flavors.me
Slide Share	Tumblr	YouTube	Pinterest	About.me	Vimeo