How to make Mobile Device Management Security Policy more effective

By Thiruvadinathan
Happiest Minds,
Infrastructure Management and Security Services

Mobile Device Management and Security - Making it more effective

Mobile communication devices are changing the way organizations work today. As more and more corporate data access and collaboration activities converge to hand-held devices such as smartphones, the line between corporate data and personal data is becoming increasingly blurred. Though laptops have been in use for more than 20 years now, securing them can still be a challenge as a tight security policy can take away most of the users' freedom. Personal use of laptops is unavoidable and preventing it can lead to employee dissatisfaction. This leads to inconsistent implementation of security policies on laptops when compared to desktops. Disabling USB ports on desktops is much easier than on laptops from a user acceptance point of view.

A win-win situation

As acceptance of the Bring Your Own Device (BYOD) trend is fast becoming inevitable, applying corporate security policies to smartphones can pose even bigger challenges. Especially, if employees use personal devices for work (BYOD), then any policy that restricts users' ability is likely to attract their resistance. Implementing a BYOD security policy offers certain distinctive advantages. The BYOD trend can potentially increase responsible use of devices. The other major advantage for users is that their personal device and data are protected for free using a robust corporate security policy and solution.

Making it more effective

Organizations are gearing up to roll out a Mobile Device Management (MDM) policy and platform in a phased manner to control associated risks better while ensuring higher business productivity.

1. An MDM policy must take into account every type of mobile device including laptops and there are solutions available for that. For example, mitigating data leakage or theft risks through encryption should be applicable to both laptops and smartphones as long as data access through such devices is allowed.
2. Policies need to be either data-centric or user-centric so that consistent security policies are applied irrespective of devices and access methods used.

3. Also, organizations can increase protection if users have to use corporate WLAN while in the office as all data traffic pass through it and provided WLAN is adequately protected.
4. Protection against virus and other malware is also a must as the devices would remain vulnerable whenever there is traffic that is outside of the MDM policy.
5. Policy enforcement needs to be reviewed more periodically than for any other policies. Exceptions to the policy need to be tracked as mobile devices have become a very lucrative target for personal as well as corporate data.

   Other areas an MDM security policy should address are enrolment, user and device authentication, password policy, segregation between personal data and corporate data, whitelisted applications, secure web access, data encryption, remote lock and back-up, removal of data during separation, etc.

CONCLUSION

Making the MDM security policy effective would be a long journey as every aspect of the policy can impact personal use of BYOD. An effective policy will also help address the challenges in regulated environments. Protection of privacy and personal data from loss, theft, disclosure and misuse must be dealt with as some of the staff will have access to these.

Data ownership, protecting the rights and interests of personal and corporate stakeholders remain the core of the policy. The user gets corporate protection for his/her personal data, while the corporate also benefits from a more security-conscious user. An MDM security policy has the potential to transform security into a more collaborative effort and a win-win deal between users and the organization.

To learn more about the **Happiest Minds Mobile Device Management & Security,** please write to us at **business@happiestminds.com**

About Happiest Minds

Happiest Minds is a next-generation IT services company helping clients differentiate and win with a unique blend of innovative solutions and services based on the core technology pillars of **cloud computing, social computing, mobility and analytics.** We combine an unparalleled experience, comprehensive capabilities in the following industries: **Retail, Media, CPG, Manufacturing, Banking and Financial services, Travel and Hospitality and Hi-Tech** with pragmatic, forward-thinking advisory capabilities for the world's top businesses, governments and organizations. Founded in 2011, Happiest Minds is privately held with headquarters in Bangalore, India and offices in the USA and UK.

Corporate Office
Happiest Minds Technologies Pvt. Ltd.
Block II, Velankani Tech Park
43 Electronics City
Hosur Road, Bangalore 560100, INDIA

Phone: +91 80 332 03333
Fax: +91 80 332 03000

United States
116 Village Boulevard, Suite 200
Princeton, New Jersey, 08540
Phone:+1 609 951 2296

2018 156th Avenue NE #224
Bellevue, WA 98007

United Kingdom
200 Brook Drive, Green Park, Reading
Berkshire, RG2 6UB
Phone: +44 11892 56072
Fax: + 44 11892 56073

About the author

Thiruvadinathan A (thiruvadinathan.a@happiestminds.com) is the Technical Director and Practice Lead for IT Governance, Risk Management, Security & Compliance services. He credits his rich experience in the field to his global clientele across industry verticals gained in the last 16 years. One of his recent achievements is having successfully led Happiest Minds Technologies to meet the stringent requirements of ISO27001 global standard.