June 2015

Lenovo Recommends 15 Steps to Reducing Security Risks in Business Mobility

A Practical Guide to Developing a Cohesive and Comprehensive Approach to Protecting Mobile and Corporate IT Assets

This checklist is designed to help you identify key steps to take to minimize the potential for security breaches and loss of data associated with mobile devices. Although every business is unique, these 15 points will provide you with a strong foundation for assessing your current mobile security plans and identifying aspects that may need more attention.

End-User-Centric Risk Issues

End-user actions play a big role in mobile security and reducing–or introducing–risk. This section focuses on IT security best practices to implement at the user level to reduce risk.

1. Train, train, train

Most end users want to do their part to address mobile security problems, not cause them. However research from the Ponemon Institute shows that unintended user error accounts for 25% of all data breaches, second only to malicious attacks. This is a direct reflection of a lack of effective training and policies that help end users ensure data security. Regular updates and more effective basic training are critical.

2. Implement a comprehensive directory of employees and contractors

One of the most difficult tasks for IT in business is to keep an accurate, up-to-date list of end users and their privileges that can be applied to mobile users. Active Directory is the most common tool companies use. While it's a capable system, Active Directory requires frequent updates and attention to keep it current.

3. Implement corporate tools for collaboration and file sharing

One of the most disconcerting mobility trends is end users putting sensitive or private corporate information in uncontrolled consumer-grade collaboration and file sharing sites such as DropBox, GoogleDrive and the like. There is no effective way to completely stop this, but by providing company-wide solutions that have IT management visibility, it's possible to protect more data. The key is giving the users an option to the consumer tools.

Most end users want to do their part to address mobile security problems, not cause them.

4. Develop links to HR systems for employee and contractor management so changes can be made in real time

The ability to generate an accurate and comprehensive IT directory is directly tied to the input from the HR and administrative systems. IT requires notification of any employee or contractor change in status so that their mobile privileges can be updated in real time.

5. Enlist end users by helping protect their private data

Rather than relying solely on policy and training, many companies are enlisting end users in their security efforts by reminding them they have important personal information on their mobile devices, and steps they take to protect corporate data also protects their own. This resonates with the vast majority of end users and helps enlist their adherence to training and acceptable use policies.

The Demands on the Devices

Mobility is fueled by a large number of different devices with various form factors. However, some common elements need to be in place across all devices to provide proper security.

6. Encryption is non-negotiable

The risk of loss or theft of mobile devices is well documented, so it's only logical to insist that any data resident on the devices be encrypted. Encrypting data ensures that data is protected from unauthorized use even if the storage medium is moved to another system. Vendors such as Lenovo offer a number of tools for automating encryption.

7. Adding IT support resources is a must

Like any other aspect of IT, mobile computing requires staff to support end users, applications and infrastructure. In a multi-device, multi-OS environment, you can be looking at one full time equivalent (FTE) employee per 5,000 devices. Whatever the ratio you decide on, these resources need to be in the budget.

8. For company provided devices, choose vendors with broad product lines

Common sense dictates that the more types of devices you have in use from different vendors, the greater the complexity in implementing mobile security. Some companies are addressing the issue by encouraging users to choose their device from a limited number of vendors. The key to making this work is selecting vendors, like Lenovo, that have a broad line of mobile devices that are attractive to end users.

9. Choose devices with two factor authentication

Mobile devices are easily misplaced or stolen, which potentially puts corporate data at risk. A simple password isn't enough to protect data because hackers have tools that can easily crack them. To fully protect corporate and personal assets, businesses are deploying two-factor authentication solutions (something you have and something you know). A good example is to use a security token or fingerprint along with a password. Built-in fingerprint readers, like those offered in Lenovo laptops, make it simpler to deploy two factor authentication.

A simple password isn't enough to protect data on mobile devices.

10. Password management tools are essential

Mobile users often have numerous personal and business applications and sites that they use regularly. Unfortunately, it gets difficult for them to remember passwords for all of them. So they tend to use the same password over and over, write down passwords or, worse, store them in a spreadsheet. This represents a huge vulnerability. Businesses are implementing password management tools, such as Lenovo Password Manager, to stop this practice and put a protected repository in place to store passwords.

11. Like it or not, IT needs some access to user devices

As more mobile users download and store corporate data, it becomes incumbent upon them to allow IT limited access to their personal devices to protect that data. In the case where a device is compromised, this allows IT to wipe corporate data from it. In just the past year we've seen substantial advances in the "wipe" function. Whereas once it cleared out the entire device, it's now possible to selectively wipe the device. Another option is to use virtualization technology so no data is resident on the mobile device, but there are some applications where this is not an acceptable solution for performance or connectivity reasons.

Protecting Corporate Systems and Data

The third area of mobile security that must be in place to insure protection, is to focus on the corporate applications and sensitive corporate data. These steps will help identify the key processes and approaches that should be considered.

12. Use virtualization and cloud solutions to reduce risk

Some corporate data should never leave the data center because it's too sensitive or entails too much risk if made available for downloading. Virtualization or secure cloud access, where data remains in the data center or cloud, can help keep such information secure. These tools may present some performance issues, but that issue may be offset by security demands.

13. Be rigorous about managing application access and privileges

Too many companies manage application access on a simple permission basis. You ask for permission, and you get it. That's not going to keep your critical information secure. At a minimum, your organization should have role-based privileges, and ideally another level of granularity based on a different metric, such as job title. And these privileges should be updated as the business changes and as employee roles change. One of the best ways to keep applications and data secure is to ensure they're only used by those who should have access.

One of the best ways to keep critical data secure is to make sure it's only used by the right people.

14. Implement Mobile Device Management (MDM)

MDM tools come from many vendors and have varying levels of security, but even basic products provide important security functions. Ensuring that you can authenticate the device, and that it hasn't been compromised or jail broken, is critical to protecting corporate data. MDM has become a necessity for managing access from employee-owned devices and provides important protection for employer-provided devices as well.

15. Document a backup and restore process

Protecting data with an effective backup and restore process is just as important in a BYOD world as it is for PCs. And the issue still revolves around having backup and restore functionality that's easy to deploy, manage and use. This is one area where Lenovo laptops and tablets are well ahead of the competition.

Conclusion

The risk of data loss and security breaches from mobile computing is substantial, whether it's lost devices, hackers gaining entry via mobile employees or the steady stream of new threats coming out. The good news is that organizations can still reap the benefits of mobile computing by combining sound security policies with end user training, intelligent device selection and by taking steps to secure their most valuable data.

To learn more, visit www.lenovo.com/smallbusiness.

Sources

- Hawthorne, Nigel. "How Much IT Support Does BYOD Really Need?" MobileIron. 19 July 2012. Web.
- Schwartz, Mathew J. "Mistakes Approach Malice As Data Breach Cause." InformationWeek. 5 June 2013. Web.

Intel Inside®. Powerful Solution Outside.