June 2015

Determining Organizational Readiness to Support Employee-Owned Devices

A checklist for evaluating key issues when allowing access to corporate data and applications by employee-owned devices

The use of employee-owned devices (EODs) within organizations has exploded. In a number of cases, the use has preceded the implementation of processes and structures to fully support them. As a result, organizations must quickly catch up. Businesses need a cohesive plan that addresses each of the key elements of supporting EODs. This checklist looks at the most important elements that will help you determine your current level of readiness to support this mega-trend, while spelling out the key processes, approaches, and best practices needed to enable it.

Foundational Policies

Policies are essential, as they document your organization's expectations about how employee-owned devices will be used. This section will highlight some of the key policies and approaches that are needed to support EODs, with better risk management and increased security for both the device and your data.

- ### Develop a Strong and Appropriate Acceptable Use Policy

  Most organizations have an "Acceptable Use" policy that spells out allowable uses of IT equipment. These policies must be updated at least twice per year, even quarterly, as new usage patterns, applications, and products emerge. A key best practice is to combine this policy with training, so that end users are aware of possible security risks. Further, many IT organizations remind users that their own personal data resides on these devices, so protecting corporate data helps protect theirs too!

Ensure IT Has Access to Employee-Owned Devices

One of the most difficult policy areas involves allowing IT departments to use tools that will give them some access rights on the EOD. This is often to "wipe" lost or stolen devices, or to provide software updates. Some corporate cultures vehemently view this practice as unacceptable, while others are more sanguine. However, if employees wish to have sensitive corporate data reside on their personal devices, it is reasonable to require some way to protect it. This is where partitioning devices is useful, allowing corporate data to reside in a specific location on the device. Using containerization tools such as AirWatch to achieve this makes good sense.

Implement Password Management

As employee-owned devices proliferate, so does the total number of personal and corporate passwords. Strong password management is therefore essential. Lenovo, for example, offers Lenovo Password Manager. This application simplifies password management, ensures that old (and possibly compromised) passwords are updated, and encourages use of strong passwords.

Employees can, and will, bring just about any device into the workplace.

Augment Employee-Owned Devices with Corporate-Provided Ones

Employees can, and will, bring just about any device into the workplace. One possible approach that can be considered is for IT to offer corporate-provided personal devices for the employees. This helps simplify EOD management and operations and provides a little more control over device usage within the organization. More organizations are providing a list of devices that they'd "prefer" employees own, often using their current PC supplier.

Deploy User Authentication Solutions

It's no secret that mobile devices can be easily lost or stolen, allowing access by unauthorized individuals. There are many public-domain hacker tools, commonly called "hammers," which can defeat systems protected with only a password. As a result, many employee-owned device programs are moving to two-factor authentication solutions (something you have and something you know). For example, this could be a fingerprint and a password. Built-in fingerprint readers, like those offered in Lenovo tablets and laptops, are a big help in implementing this important security step.

Support for Critical Security Tools

Even though your organization doesn't own the device, it's essential for it to interact with key security tools. Such tools include Mobile Device Management (MDM), a virtualization solution such as Stoneware webNetwork, or basic anti-virus/anti-malware products. Some organizations are looking to cut down on the number of supported mobile device platforms to ensure that chosen tools work efficiently on their employees' devices.

Built-in fingerprint readers are a big help in implementing mobile device security.

Reduce the Number of Vendors to Simplify Security and Operations

As discussed above, in a small- or mid-sized organization, unfettered use of employee-owned devices would likely result in "one of everything" on the network. To improve efficiency, some organizations are attempting to restrict the number of devices they support by limiting the choices on company-provided devices to a smaller number of vendors that offer a broad product line. This gives the users choices, yet simplifies support issues by focusing on a few suppliers. Lenovo is a good example of a single vendor with a broad range of laptops and tablets, providing consistency across the range of EOD products. This results in fewer unique security and management tools, which can substantially reduce the amount of IT resources needed for secure operation.

Simplify Patch Management

While all operating systems need patches and updates that provide important security or performance enhancements, many users ignore them. As a result, organizations are looking to improve and simplify patch management to prevent the task from devouring scarce IT resources. Tools such as LANDesk Patch, which is provided with Lenovo devices, can be invaluable for automating and simplifying the deployment of patches. However, the tools for non-Windows tablets and smart phones are in their infancy.

Managing the Employee-Owned Device

Just because these devices are not corporate-owned doesn't mean that they don't need management. In fact, because they can leave with ex-employees, management tools are critical.

Just because these devices are not corporate-owned doesn't mean that they don't need management.

- ### Document and Reduce User Application Access

  Some organizations allow users wide access to numerous applications, some of which may not be necessary for them to complete their job. This practice often presents more vulnerability, and reducing unneeded access should be part of your EOD plan. While it is simpler to have fewer sets of permission policies for application access to deal with, this small efficiency isn't a good trade-off in the world of employee-owned devices. Limiting application access is the first step to reducing potential misuse.

- ### Put IT Resources in Place to Support the Users

  The productivity gains from EOD are substantial. However, all of this capability also demands IT support. Most IT organizations do not have the extra bandwidth, let alone the expertise necessary to support a huge and widely-varied population of new devices. Therefore, adding resources is almost always necessary. Scrimping on IT resources will cause problems that negatively impact productivity and cause user frustration. It is worth noting that some businesses are subtly pushing end users to corporate-provided devices, with the promise of better and faster support.

- ### Implement Mobile Device Management Tools (MDM)

  MDM tools provide the first layer of security and manageability for supporting employee-owned devices. MDM has four key functions for dealing with employee-owned devices: securing, monitoring, managing, and support. MDM tools also ensure that devices connecting to your network meet specific security requirements.

- ### Develop a Role for Virtualization

  One of the most effective approaches to protecting corporate data and applications is to only run them "virtually" on the employee-owned device. Using virtualization and secure cloud access tools like Lenovo/Citrix VDI or Stoneware webNetwork keeps the corporate data in the data center, ensuring it is protected. Virtualization may not be appropriate for every application or use, but it is a very strong option where it can be used effectively.

Information Security

In addition to managing the devices and information residing on them, there are specific security requirements when dealing with employee-owned devices. For example, there are two "modes" where you need to ensure that information is protected, "in flight" and "at rest." Both are an essential part of securing data on employee-owned devices, as your information can be at risk on public networks, or taken from lost/stolen devices.

Encrypt Local Device Storage

This is most likely the single most important aspect of data protection for employee-owned devices storing corporate data. It is not unusual for these devices to be lost or stolen, and encryption helps to ensure that data on them is protected from hackers and thieves. Choosing products with strong encryption options like Lenovo's tablets and laptops is critical to successfully protecting mobile devices.

Use Cloud Services to Secure Data

Many cloud services offer encryption options for data that is in flight and at rest, to provide a "safe" environment. In cases where the time and cost of upgrading or implementing new internal IT EOD security solutions is too difficult or not in the budget, cloud services to support EODs represent a good solution. Tools such as Stoneware's webNetwork secure cloud access solution add another layer of protection for cloud-based applications and data.

There should be protection for any corporate data flowing through a public network.

Implement Public Network Security

Most employee-owned devices use public networks for communication with corporate systems and infrastructure. This poses potential problems. The old "tried-and-true" VPN solution is often the starting point for security when employee-owned devices use these public networks. The encryption of network traffic can also be done using software solutions from firms like Symantec or Cisco. Regardless of the approach, there should be protection for any data flowing through a public network. A side note that needs to be addressed here is the need for user training about fake hotspots. Users must be wary of public WiFi that may not be legitimate. These fake hotspots are set up by hackers with network names such as "Free WiFi" or "Airport Network", allowing them access to data you are sending and receiving.

Protect Corporate Data Used in Collaboration Tools

Protecting corporate data has two aspects. First, there's training, which must address acceptable use of such collaborative file-sharing tools as DropBox, GoogleDrive, Box and similar services. Some organizations are going further and replacing these consumer-focused and difficult-to-secure data sharing tools by standardizing on, and providing corporate tools such as Office 365, which allows IT management full tracking and visibility on data sets that are being shared so that they can stay secure.

Summary

There are numerous aspects that impact an organization when employee-owned devices are allowed into the IT environment. The process for supporting them combines new devices with the security, access, and policies essential to using them responsibly. However, each organization has its own unique issues around the use of these devices, and securing corporate data and applications. It is also important to note that EODs are a very liquid trend, and changes happen constantly. It's worth revisiting your approach on a regular basis.

Master this topic with more information on this topic and other mobile security issues at www.lenovo.com/smallbusiness.

Sources

- Acohido, Byron. "Security for Personal Mobile Devices for Work Tightens." USA Today. Gannett, 7 Jan. 2013. Web.
- Bailey, Don. "Insider Threats And Employee-Owned Devices Identified as the Greatest Risks In The State of Network Security 2013 Survey." Dark Reading. 17 Apr. 2013. Web.
- "Data Breach Trends & Stats." In Defense of Data. Symantec, Dec. 2011. Web.
- Olavsrud, Thor. "4 Mobile Security Predictions to Help