Tech Tip

Is that Smartphone a threat to your organization?

Your trusted employee brings in their new iPad and wants you to set up their email and server access on it. They attend a lot of external meetings and it would be convenient for them to have mobile access. Sounds like a simple decision.

* What if that device is not password protected and it gets lost or stolen?
* What if that trusted employee transforms into the crazy, enraged employee and leaves the organization?
* You can change passwords and stop them from accessing beyond that date, but you don’t know what they’ve saved on their device.

In a world where seemingly everyone has a device that they bring everywhere, how can you make this work for your organization while keeping your IT infrastructure and important data from being accessed by malicious entities?

A **Bring Your Own Device (BYOD)** strategy can be the answer.

According to a study by Microsoft, over 67% of employees at surveyed companies bring their devices to work, regardless of their company’s policy. Based on this statistic, it would seem as if a Bring Your Own Device strategy would be a no-brainer, but there are many variables to consider.

In order to begin to design a BYOD policy that works for your company, you will have to determine the elements you are trying to protect, the access employees have to those elements, and how to react when you need to enact the protocols of that policy.

Ask yourself these questions:

* **Does increased mobility benefit the organization?** The ability to reach beyond your network and still access all the work-related material can be an indispensable factor for the modern employee. People are busier than ever and often need to multitask just to get by.
* **What are the risks?** You’ll also need to understand what threats are inherent by allowing foreign devices to access your network, as well as the issues that come with allowing your data, the lifeblood of your business, to be accessible on other networks. With sensitive data breaches costing companies thousands of dollars, can your organization sustain itself if you were put in that unenviable position?
* **Do you have an Acceptable Use Policy?** This policy governs what content is available to people on your network. In this policy you are able to set forth what is off-limits to the end users. There is a fine line between adequately protecting data and restricting access in a way that decreases productivity. The purpose of an Acceptable Use Policy is to define that line.
* **Are you ready for tough decisions?** Many mobile device management strategies include an option to wipe-clean a device of a user that has left the company. This is generally something that the user must agree to prior to connecting their device. However, most users would rather remove the company data voluntarily than have their personal device wiped clean. In what situations would you use this?

Considerations when designing your BYOD policy:

1. Specify which devices will be permitted on the network.   
2. Establish a static and comprehensive security strategy.  
3. Define how foreign devices can access data on the network.   
4. Ensure staff knows who owns what on the mobile device.  
5. Make a decision on what kind of use to ban on foreign devices.  
6. Combine your BYOD strategy with your acceptable use strategy.  
7. Create a strategy to quickly and securely on-board and remove users.

Your BYOD policy needs to fit your organization and ensure that the security of your data isn’t compromised.