Things to Consider Before Deploying a BYO Strategy

Over two thirds of Americans have a smartphone, almost half have a tablet. And many companies are implementing BYO programs. There are many things for a company to consider before deicing on a BYO program. First there needs to be a thorough understanding of the BYO programs available from which a company can choose. The four types of programs companies can choose when dealing with devices and employees: BYOD (Bring Your Own Device), CYOD (Choose Your Own Device), CLEO (Corporate Liable Employee Owned), and COPE (Corporate Owned Personally Enabled). Each type of program has its own set of advantages and disadvantages.

There are also questions that need to be considered in order to determine the appropriate program. Things like who owns the device? Who will maintain the device? Who owns the data? Who is paying for the bills and accessories? And who owns the phone number associated with the device? Each of the four BYO programs will have a different combination of answers. For example, in a traditional BYOD program, the customer owns the device and number, but what about the company data? What if the phone is lost or the employee no longer works at the company?

Understanding the implications of each program is paramount in choosing the right one for a company. Before choosing a program, there are five areas of considerations that should be thoroughly examined: policy, risk assessment, IT security, deployment and support.

Policy: This is where most programs need to start because there must be procedural protocols in place to protect both the employee and employer by defining the terms and limits of the program. A good BYO policy will not only specify which BYO program is in place, but also the rules surrounding the level of support for company or employee-owned smartphones, tablets, and laptops. The policies will also define the parameters of data security, who owns the data regardless of who own the phone, how deployment and maintenance will be handled, and also the security protocols during emergencies. Topics like who will pay for the phone, what which budget from which department, and who will be responsible for maintaining and upgrading the phones should also be established in the company policies. Establishing good policies and procedures at the beginning also cuts down on company legal fees. Company policy should be the first step in considering which BYO program may be right for a company and will effect the other four topics of consideration as well.

Risk assessment: Risk assessment requires looking at the components in on organizations infrastructure to identify potential vulnerabilities and how to management them as they apply to a BYO program. It is important to understand the risks associated with each type of program before deciding which plan to use as each program has a different pros and cons that will impact the company and the level of risk that is acceptable. Bring Your Device (BYOD), for instance, has a different risk level than the hybrid Company Owned, personally Enabled (COPE). For instance, with BYOD, each employee brings their own device, so other family members may use that device, or there may be applications that compromise sensitive company or client information. That level of risk seriously impacts any business, especially in the medical or financial industries that have stringent privacy regulations. For information that is highly sensitive, and industries with more robust data security requirements, COPE program may be better because risk mitigation is much lower. Companies will need to determine the risk tolerance not across on enterprise, but also for their perspective industry, as some industries have stricter guidelines for data and client information.

BYOD, CYOD and COPE, CLEO programs

IT Security: A large part of implementing any BYO program will be IT and security. This goes hand in hand with risk assessment. It is important to understand how to navigate the vulnerabilities and limitations of a company's infrastructure when choosing a BYO program. Each of the four programs have different security and data risks. Bring Your Own Device will have many different risks associated with it because of the numerous devices that could be brought in, and even more applications that must be addressed and secured. CYOD (Choose Your Own Device), where a company limits the devices that can be used, will have fewer IT security issues because there will be fewer devices in action. A more secure option might be a CLEO (Corporate Liable Employee Owned) program, where the company places it's own applications to on an employee owned phones. Those applications are secure, but since the employee still owns the phone, there are still risks of breaches is data security. For buniesses and industries that need the highest level of security, COPE (Corporate Owned Personally Enabled) nay be the best because it allows a company to have complete control over what applications and information is on the phone and what type of access will be granted per phone. A company can limit which applications b]can be downloaded, and can wipe the phone should it be lost or if the employee leaves the company without returning the device.

Deployment: How the devices will be deployed also must be determined. Deployment can be costly and time intensive, burning through budgets if not properly planned and carefully implemented. Which phones, tablet or computers are compatible with the networks and infrastructure? What applications need to be used, and what if any, are the memory or other requirements of the devices that are to be connected? If many different devices are allowed into a BYOD program, then IT may be spending time with connectivity issues. There also may be different compatibility issues with older devices.

Support: If not properly thought out and implemented, supporting a DYO program can prove very costly and cumbersome. BYOD may be one of the most popular programs, but it also requires a lot of support because of the wide variety of devices that will be used and connected into the company. It is not just an issues of Android or Apple, it will be having an IT department that not only understands the limitation and capabilities of each type of device, but also how those relate to the company infrastructure and network. Support and trouble shooting may be more manageable with a (Choose Your Own Device or a Corporate Owned Personally Enabled program. The latter of the two programs will limit the choices the employee has, but it will make support easier because of the limited amount of devise involved. It will also benefit the employee because they are given a device that they can use as needed at a discounted rate.

As with any business decision, choosing a BYO program needs to be well thought out and managed. With the proper planning, the rollout, deployment, and support will be smooth and efficient.