Acronis

BRING YOUR
OWN DEVICE

Driving Workforce Productivity with Bring your own DEVICE (BYOD)

Introduction

With over a billion smartphones and tablets at arms length, a majority of your global workforce already possesses the technology needed to better connect them to the corporate network. Widely known as the "consumerization" of the Enterprise Workforce, facilitating the connection of these personally owned devices could decrease the costs of maintaining corporately-liable devices, improve productivity and collaboration, enhance the work-life-balance environment and even foster innovation.

Unfortunately it is not as simple as allowing employees to connect to the enterprise Wi-Fi and therefore companies moving toward a BYOD program must understand the risks and the protective measures needed to secure these devices. Technologies and policies are required to avoid inappropriate use, mitigate against loss of data and intellectual property as well as defending from attacks of malicious parties and software that will now have more access points in to your network.

This white paper will discuss the benefits of deploying and embracing a BYOD program and areas to be considered to adequately protect your company and its critical data and file assets.

PERSONALLY OWNED DEVICES ON YOUR NETWORK

As BYOD programs evolve and consumerization continues, employees are empowered to choose a device or devices they feel are best for them to get their work done. This includes smartphones, tablets and hybrid laptops. With these devices, people can become more mobile and productive.

They are no longer constrained to the office and therefore can be closer to their remote counterparts as well as your customers. Equally as important, a more satisfying work experience helps organizations recruit and retain the best employees as they have a greater sense of control and freedom over their preferred technology. Additionally, by shifting device ownership to employees, "IT" eases its burden for endpoint asset management and administration.

The merits and attractiveness of BYOD are easy to understand.

1. **BYOD Increases Productivity –** Many companies that have already adopted BYOD have seen a noticeable increase in employee productivity. They also believe they would face competitive disadvantages by preventing BYOD. Why? Employees who use their own devices at work also tend to spend more time working remotely. When you have the same device on you at all times, the barrier between work life and personal life starts to blur. Simply put, BYOD programs give employees the ability to work offsite, and thus increases productivity out of the office.

2. **BYOD is the Future –** It doesn't matter whether your company thinks BYOD increases productivity and saves money, because people will bring their own devices to work no matter what you do. Even if, for some reason, you decided that you absolutely didn't want people bringing their own smartphones to work, how would you implement such a policy? You can't tell people to just leave their phones at home all day. That's not how people expect to communicate with each other. Job satisfaction would plummet and a lot of excellent employees would go work for your more open-minded competitors. It's better to embrace the inevitable.

3. **BYOD Provides Flexibility –** Mobility has blurred the lines between work and personal life as well as geographic lines. Mobile phones, tablets, and similar devices make it cheap and easy for someone in Australia to do business with someone in the United States.

Yet with all of its positives, there are inherent risks and drawbacks to BYOD. With BYOD, the number, type and geographical distribution of endpoints increase significantly. There are increased security and manageability issues that are now introduced. Without proper controls (technology and polices), these personal device endpoints could potentially infect the company network with viruses, and private customer or company data can be compromised if the device is lost or stolen. Employers also risk becoming unwittingly responsible for liabilities beyond their control: corporate assets might get mixed with personal data such as family photos and music or, worse yet, with downloaded applications that are not safe or in line with company policy.

Therefore, before enterprise leaders embrace a BYOD initiative, there needs to be plenty of due diligence expended looking at their own internal operations in order to assess the extent and impact of deploying such a program. The ultimate goal is to implement a BYOD program that supports device diversity while putting the proper safeguards in place to keep business assets safe and personal items separate.

THE FUTURE OF BYOD

Under the guidance and direction of the C-Suite and IT leaders, an Enterprise Office of Mobility should be established to lead the analysis and planning of implementing an Enterprise-wide BYOD strategy. This team should have representation from IT, the Business, Legal, HR, Operations and Sourcing/Procurement at a minimum. A team that represents all facets of your Enterprise in order to best study and plan for the impact of a pervasive change and computing policy.

End users of a BYOD program expect seamless functionality from the start, and it is difficult to recover from even small glitches in the initial rollout. And after control over access to digital assets is given away, it is hard to take back. In other words, there is one chance to get BYOD right, so it is important to have a detailed strategy and design in place before the project begins.
A good place to start the planning is to update/document the Enterprise Security and Information Architecture. This will help assess appropriate and inappropriate points of access by personal devices.

Network segmentation and expansion are often required to properly support a BYOD program and endpoint security facets are also a key success factor. Ensuring that there is an understanding of what is in place will aid in locking down what areas should not be accessed due to risk of data loss or network penetration by unwanted parties and malicious software.

As for the physical devices, diversity is a huge part of a BYOD. There will be numerous device types and mobile operating systems chosen by your employees and therefore, IT will need to be prepared to support the devices that have been approved for access and use on the corporate network. Setting a standard on device types and operating systems will allow for the highest opportunity for success by IT in managing such a mobile strategy.

While you are evaluating the organization and preparing your implementation plan, start thinking about future BYOD policies and guidelines. Beyond the standard policies for monitoring activity and enforcing security, consider what defines acceptable use and what will happen if the device is damaged, lost or stolen. For example, what should a BYOD user do if their device is compromised or misplaced? Where should they report this type of situation and within what timeframe? And what, by policy, will happen to the corporate side of their devices as opposed to their personal content. Users must understand their responsibility to remain productive.

Equally as important as detailing the responsibilities of the BYOD end user, the Enterprise needs to ensure clarity of what levels of control and access they have over the personal aspects of the employee-owned device. For example, if a employee’s personal device needs to be removed from the BYOD program and a “device wipe” of corporate assets from the device is required, what assurances does the employee have that personal content will not be deleted. Standards and guidelines provide for the information needed for an employee to trust that a BYOD program is not going to negatively impact their personal lives.

Also, policies will detail the extent of control that the Enterprise has over the personal device and property of the employee. There is a natural trust-gap that only adequate levels communication and policy structure can bridge.

THE IT COMPONENT OF BYOD

Often, the Enterprise will need to retool current IT employees to better understand, administrate and support these new mobile devices and access points. Therefore, training, new equipment and enhanced service level agreements for support are all recommended for IT personnel to properly deploy and operate the BYOD program. Furthermore, Mobile Device Management (MDM) and Mobile Application Management (MAM) should be considered. As stated before, it is not as simple as allowing for Wi-Fi connected devices on to your network. Solutions are needed to manage what devices are allowed to connect and what applications are allowed to access the network by BYOD subscribers.

Equally as important as MDM and MAM, Mobile Content Management (MCM) is critical to the success of a BYOD initiative. After all, without access to vital content like desktop files and network shared drives (documents and data), then simply having a device connected to your network will yield very little positive outcome. The ***Acronis Access Advanced*** solution enables enterprise employees using any device to securely access, sync and share corporate content while IT maintains control over security and compliance. Content can be accessed from file servers, NAS, SharePoint, and personal devices, and shared with approved internal and external constituents. ***Acronis Access Advanced*** empowers IT to control the level of security needed via the same Activity Directory solution used to managed user accounts and access privileges already being used for corporate email and content repositories (SharePoint and network drives).

CONCLUSION

Trends like device consumerization, desired workplace flexibility and cloud computing facilitated by BYOD programs will continue to transform the way people and organizations work. The right strategy, enabled through the delivery of on-demand content and data with access to the latest Enterprise mobile applications to any device anywhere, will:

- Empower your employees;
- Increase workforce productivity and geographic reach;
- Improve collaboration with co-workers and customers; and
- Reduce costs and simplify IT management.

Acronis

About Acronis

Acronis sets the standard for New Generation Data Protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe backups of all files, applications and OS across any environment—virtual, physical, cloud and mobile.

Founded in 2002, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products have been named best product of the year by Network Computing, TechTarget and IT Professional and cover a range of features, including migration, cloning and replication.

For additional information, please visit **www.acronis.com**.
Follow Acronis on Twitter: **http://twitter.com/acronis**.