Insight

Achieving a BYOD (Bring-Your-Own-Device) Strategy That Works for You

Learn Five Steps to a Successful Strategy

In many circles, BYOD no longer needs to be defined. It has become shorthand for a prominent part of a phenomenon known as the “consumerization” of IT, where technology innovations from the consumer market proliferate into business and government organizations, breaking the traditional IT department top-down control model.

While some IT professionals recoil at the thought of allowing employee-owned devices to burrow into corporate networks, more and more of them realize that a BYOD strategy can result in quantifiable benefits as well as increased employee collaboration and productivity when properly planned, implemented and managed.

The *Cisco IBSG Horizons Study* (May 2012) of 600 U.S. IT and business leaders shows that 95% of organizations already permit employee-owned devices in some way, shape or form in the workplace, and 76% of these IT leaders consider consumerization of IT “somewhat” or “extremely” positive for their companies. The leaders in this study may be the vanguard, but according to Gartner’s report *Opportunities and Conflicts Loom in the Wake of Google’s Motorola Mobility Deal* (October 7, 2011) they predict that by 2014, 90% of organizations will support corporate applications on personal devices--and this isn’t just a single device per employee. The Cisco study concluded that the average number of connected devices per knowledge worker is expected to reach 3.3 by 2014, up from an average of 2.8 in 2012.

BYOD Changes the Landscape

By implementing a BYOD strategy, organizations empower their employees. At the same time, IT departments are forced to make major adjustments in order to support the strategy. Rather than support a predictable set of standard devices and applications, they must now cope with rapidly changing hardware, operating systems, applications, and even an array of service providers and plans. Increasingly, their approach must be to guide and influence rather than to dictate and control.

Since the value of these employee-provided assets is to connect to the corporate network and increase productivity, it exposes IT departments to even greater challenges. Allowing uncontrolled access to corporate resources is extremely risky. Organizations need to provide appropriate access to authorized personnel. At the same time, they must prevent unauthorized access and ensure that unlicensed or inappropriate content, applications or malware on the employee’s device doesn’t infect the organization, create breaches of sensitive data, or expose the organization to liability - a tall order indeed.

BYOD Strategy

The risks associated with implementing a BYOD strategy cannot be addressed just by implementing a Network Access Control device such as a firewall, or simply by developing employee rules or policies. To ensure security, compliance, and data protection, companies need to develop a seamless, integrated mixture of policy and procedure, network infrastructure and resources, and process and management. All of these factors must be easy to understand and use by the range of employees and flexible to meet their needs.

The key to a successful BYOD strategy is maintaining a balance between the organization, the user and the device with security, access control, and organizational policies. In order to achieve this balance, organizations need to develop granular access policies, automated policy enforcement, have visibility into the devices, and insight into the user profiles and their needs.

Steps to a BYOD Strategy

1. Establish a baseline. Review where you are and where you are going.

Review and update corporate policy and procedures. Consider not only what the organization has encountered but anticipate potential threats and opportunities.

Review current network status and determine the one-to-three year vision for network infrastructure such as: wireless LAN (WLAN) and VPN (Virtual Private Network) connectivity, network services like security, quality of service and bandwidth requirements, applications, data storage and access, and asset and network management.

Determine if additional resources will need to be acquired or reconfigured to support an influx varied wireless devices without throttling bandwidth, creating bottlenecks, or port contention. Learn what it will take to authorize and register employee devices on the network and into applications. Network and mobility assessments may be helpful in establishing an inventory of current network resources and devices. Network and infrastructure impact assessments and remediation planning can avoid unexpected expenditures or budget surprises.

2. Review your current security posture, potential gaps, and emerging threats.

Security policy, procedures, and standards are not just statements on paper, but must be operationalized and made real. No binder of security policies will defend an organization against public opinion if a hacker releases private customer financial data. Cisco Security Intelligence Operation releases an *Annual Security Report* and a periodic *Cyber Risk Report* that highlight trends and emerging threats. Some organizations or even departments within organizations are subject to more stringent demands such as regulatory requirements on financial disclosures and or compliance with government or industry standards. The IT department needs to act in an advisory role to these other disciplines to ensure they are aware of areas of risk and vulnerability and what they need to do to mitigate those. It must ensure ongoing security monitoring and cyber safety management.

3. BYOD requires a shift in perception; the individual is the endpoint.

What employee groups or user profiles need access? What types of devices will they have or need? Smartphones, tablets, notebooks, employee personal computers, e-book readers, gaming consoles: the lines between these devices are blurring. What privileges or permissions do they need? What applications? Where are they located (office, home, road) and when will they need access or resources? Will they need email from home, ability to calendar meetings on a mobile phone, initiate web conferences, access the corporate directory or intranet from a hotel, place an order into a point of sale system, run an HR report or initiate end-of-quarter financial reporting? What integrations are required? What's the best way to engage employees to accommodate necessary modifications to their devices for security such as encryption or authentication?

4. Inform and educate

Now is the time to educate employees about the reasoning behind the BYOD policy along with the fact that ***it is*** going to be enforced. It is very important that employees are aware of this for the implementation to be successful. Unfortunately, employees bring on a majority of security issues because they are unaware of the policy or choose to ignore or actively circumvent it.

Educating employees is especially imperative as the so-called Internet Generation enters the workforce. According to a Cisco *Connected World Technology Report*, seven out of 10 young employees frequently ignore IT policies, and one in four is a victim of identity theft before the age of 30. The report goes on to state that “the desire for on-demand access to information is so ingrained in the incoming generation of employees that many young professionals take extreme measures to access the Internet, even if it compromises their company or their own security. Such behavior includes secretly using neighbors’ wireless connections, sitting in front of businesses to access free Wi-Fi networks, and borrowing other people’s devices without supervision…considering that at least one of every three employees (36%) responded negatively when asked if they respect their IT departments, balancing IT policy compliance with young employees’ desires for more flexible access to social media, devices, and remote access is testing the limits of traditional corporate cultures.”

5. Adapt and evolve

Regularly examine your BYOD strategy. Build in provisions to test, tune, and trash as needed. Be proactive in looking for emerging trends that will either positively or negatively impact your plan. Monitor usage and plan for growth and expansion.

By addressing the above steps, you will have developed a granular BYOD policy. By providing a granular policy definition, it becomes easier to automate enforcement by implementing a Network Access Control solution such as the Cisco Identity Services Engine (ISE). If a situation occurs where an unidentified user attempts to access the network, automated policy enforcement enables the ISE to either reject the attempt or assign the user to a guest profile that has fewer privileges, such as Internet access only, and it can deny access to other network resources such as back-end servers.

Insight Enterprises, Inc. is a leading technology provider of hardware, software and service solutions to business and government clients in North America, Europe, the Middle East, Africa and Asia-Pacific. Insight is focused on helping organizations move technology goals forward in the areas of Cloud, Virtualization, Data Center, Unified Communication & Collaboration, Networking & Security, Data Protection, Mobility & Point of Sale, and Office Productivity. Insight’s goal is to be a trusted advisor guiding clients through the entire Information Technology lifecycle and acting as an extension of the client’s team to realize innovative technology solutions.

For more information about BYOD Strategy and Insight’s Mobility Solutions, please visit **http://www.insight.com** or contact your Insight rep or call **1-800-467-4448.**