

Enterprise 2.0 – The Next Generation, Mobile Enterprise

With the barriers of traditional enterprises breaking down, CIOs must prepare to support a progressive workforce and trends such as bring-your-own-device, virtual desktop environments and the cloud.

In 2012, the continued consumerization of IT spawned a series of trends — bring-your-own-device, virtual desktop environments and the cloud for example — that have begun breaking down boundaries of the traditional enterprise. The result is Enterprise 2.0, a mobile enterprise that is changing the face of federal IT.

One of these trends, bring-your-own-device (BYOD) illustrates this disintegration of enterprise boundaries as thousands of employees in the public and private sectors went to work asking to use the same devices in the office or in the field as they did at home. According to research firm International Data Corporation (IDC), the growth of BYOD is set to accelerate, with sales of smart mobile devices such as tablets and phones expected to grow 20 percent in 2013. In the public sector, BYOD has been further bolstered by the Telework Enhancement Act of 2010 and the Obama Administration's Cloud First initiative.

These cultural and governmental IT trends have combined to present several challenges for federal IT managers, who must prepare their infrastructure to incorporate not only mobile devices but also virtual desktop and cloud technologies. "IT's best strategy to deal with the rise of BYOD is to address it with a combination of policy, software, infrastructure controls and education in the near term," according to a recent report from Gartner titled Bring Your Own Device: New Opportunities, New Challenges¹.

When dealing with Enterprise 2.0 and all that it entails, CIOs might look at these challenges from three perspectives: technology, culture and acquisition strategy.

Getting technical

Perhaps the most important change with Enterprise 2.0 is that the reach of the enterprise has been extended. For many years, it was confined to networks and systems inside an agency's buildings and data centers. These "walled gardens" enabled closed communities and rigorous controls existing within very tightly controlled security boundaries. With BYOD, however, such boundaries are practically non-existent, as federal workers are accessing information and services from far afield, down range locations and home offices. Information now needs to be accessed anywhere, anytime by a dynamically changing user population.

That has serious ramifications when it comes to cyber security, which must be pushed out all the way to the "edge" or end point, where the user is actually interfacing with the network on their mobile device. The IT department must find a way to securely deploy and control that end point, whether it is a tablet, phone or home PC. This strategy creates new challenges, but also opportunities to design improved network and data center architectures to ensure security is built-in to the total information ecosystem including the end points where agencies access data to support their missions.

BYOD means IT must re-think the traditional security paradigm to enable higher risk activity to occur on the network while not compromising important security requirements. Agencies must investigate strategies such as segmentation and other ways to look beyond the traditional network boundaries to ensure that these diverse end points can securely access information and applications in the data center.

¹ <http://www.gartner.com/it/page.jsp?id=2136615>

One emerging data center capability that enables this kind of secure access is virtual desktop technology, which enables IT organizations to provide secure access to data within the data center in a manner that can reveal information based on how and where the user is accessing data.

Another significant data center capability is the emergence of web and cloud based technologies such as Application Storefronts, Mobile Device Management and the Intelligence Community/ Department of Defense's Ozone Widget framework. These technologies put more power in the hands of both developers and users to create lightweight applications accessing centralized data center information stores.

All three pieces – security, network and data center strategies – are tied together. When considering implementing these new technologies agencies need to assess the impact to multiple layers of their enterprise. This will increase operational success and reduce security risks when launching a BYOD or cloud strategy.

Changing the cultural landscape

With any new technology deployment, it is best to begin by understanding the goals of the program or organization – What are you trying to do? Are you looking to offer greater agility? Or are you looking to drive cost savings? And how can you do that and also meet the needs and desires of the workforce?

Once that is clear, it makes it easier to align IT with those goals and to identify the cultural changes that will be involved. This is a case where virtual desktop infrastructure (VDI) can help. By implementing the technology on tablets and mobile devices, the IT department can control how data is accessed. Second, since data resides on the server, not the device, it is much less susceptible to being compromised even if users are careless.

Within this next generation, mobile enterprise both BYOD and cloud are seen as game-changers for the end user, providing them with much improved access to the resources they need wherever they might be working. That said, IT must mesh end user expectations with their agency's security and access requirements. That involves evaluating the work patterns of employees, contractors and partners, and understanding how they want to use this technology to work outside the enterprise.

For example, General Dynamics has developed a private-cloud application for access to intelligence data using a Data-as-a-Service model, where users can access information using traditional desktop computers, virtual desktops, thin-clients, tablets or smartphones. This flexibility provides the user with the ability to configure information access based on mission needs, but centralizes the information storage and security so that end user devices are not polluted with sensitive or classified information. This provides both user flexibility and data protection.

IT managers also need to look at existing acceptable-use and other IT policies that govern end user devices. Particularly with BYOD devices, agencies should consider having a legal expert review all such policies and identify any potential problems. For example, if an employee is storing agency data on a personal device, does the organization have the right to confiscate it if there's a question or problem? If so, how must sensitive personal information, which might also be on the device, be handled?

Agencies also need to decide whether to mandate the use of anti-virus and anti-spyware on those devices. As a rule, IT managers need to make sure they provide clear policies and guidelines on the use of all devices, whether government- or employee-owned.

Smart mobile acquisition

The final piece of the puzzle for organizations grappling with BYOD is acquisition. Most existing acquisition policies assume that the government owns all of their IT assets and that those assets remained with the organization until they reached end-of-life. That is not the case with BYOD. While they avoid purchasing hardware and device, agencies still might share the cost of service and support.

This hybrid model requires a shift in thinking. Agencies first must understand how to acquire service-based solutions, which in itself is a significant challenge. Then they must figure out how to work with the mission side of the agency to develop requirements for these acquisitions and to ensure that they comply with "Cloud First" and other federal initiatives. Also, many IT departments are still struggling to demonstrate the return on investment of the services-based approach to mobile or cloud solutions.

Agencies also might find their options limited when it comes to customization. Federal agencies often ask vendors to customize their products to meet unique government requirements. But with BYOD, in which employees buy off-the-shelf devices and tablets, customization must come after the fact. Even those devices that are purchased by the agency may not be customizable. Instead, agencies will need to work with providers that can create apps, security features and services designed specifically for them. Long term this provides additional value by creating a modular ecosystem built from standard components of commercial solutions tailored to meet the specific needs of the agency rather than customizing specific solutions. Over time this reduces cost and complexity along with increasing the security posture of the information management life-cycle.

What should organizations be doing?

When it comes to Enterprise 2.0 and a mobile workforce, incorporating BYOD, virtual desktop technologies and cloud into your strategy can seem daunting. However, preparing for these challenges and taking the necessary steps to deal with them will make the transition that much easier.

The recommendation now is to explore adopting the commercial model where those agencies that have deeper requirements can purchase devices and trust valued partners to build an ecosystem that supports what they need. If you are exploring implementing a VDI solution consider including the broader ecosystem that supports a VDI such as security, network impact, the end user use case and access the infrastructure and applications portfolio. Considering these factors improves the quality of the end user experience and increases your agencies success in implementation.

General Dynamics Information Technology

General Dynamics Information Technology serves as a leader in cloud computing and virtualization migration and support. We assist our defense, intelligence, federal civilian and commercial customers with developing cloud strategies, building virtualization and automation solutions, choosing appropriate cloud services

and managing the current cloud computing environment. The company provides the full spectrum of services from architectures, design and development to integration and operations and maintenance for a true, one-stop shop to provide the service levels customers demand. With approximately 21,000

professionals worldwide, the company manages large-scale, mission-critical IT programs delivering IT services and enterprise solutions for customers in the defense, intelligence, homeland security, health, federal civilian government, state and local government and commercial sectors.

For more information, please visit: www.gdit.com

GENERAL DYNAMICS
Information Technology