Enterprise Strategy Group | Getting to the bigger truth.™

ESG Brief

You Must Modernize Protection When You Modernize Production

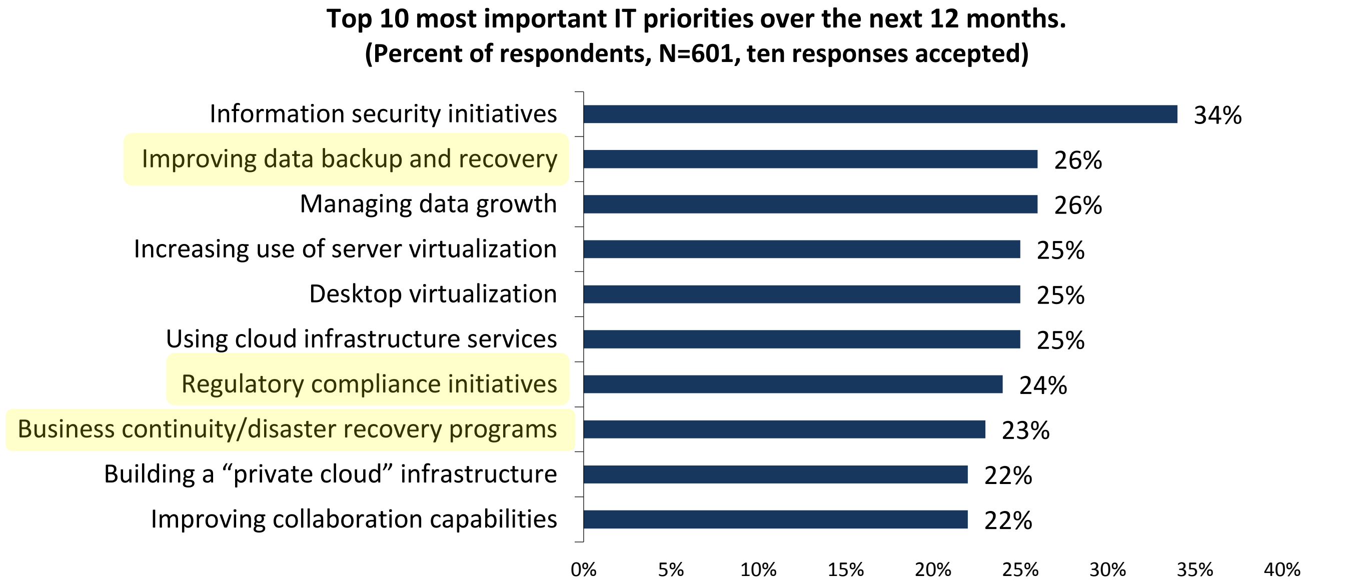
Date: March 2015 **Author:** Jason Buffington, Senior Analyst

Abstract: *Two particularly interesting data points from ESG's 2015 IT Spending Intentions Survey tell a story that is grounded in two important realities related to what is driving data protection modernization.*

Modernize Protection When You *Modernize Production*

Three of the top ten IT priorities for 2015 reported by respondents to ESG's most recent annual IT spending intentions survey relate in some way to modernizing data protection. Improving data backup, regulatory compliance, and business continuity/disaster recovery (BC/DR) preparedness were all mentioned as priorities among respondents from IT organizations of all sizes (see Figure 1).[1]

Figure 1. Top Ten Most Important IT Priorities for 2015



Source: Enterprise Strategy Group, 2015.

Another revealing finding related to IT priorities centers on organizations' efforts to modernize *production*, including their priorities to:

- **Manage data growth**, a job that entails increasing their current storage solutions' capacity incrementally or adding new storage platforms. Both will affect data protection strategy, either by requiring scale increases within the data protection storage framework or necessitating the acquisition of new backup/snapshot technologies.
- **Increase use of server virtualization**, which definitely will drive changes in data protection, including either having to upgrade from legacy backup products to

MOST IT PROS would probably never modernize their protection capabilities … unless some external forcing function was "making" them do so.

[1] Source: ESG Research Report, *2015 IT Spending Intentions Survey*, February 2015.

current versions that support hypervisor-based protection, or having to add a hypervisor-specific backup solution to supplement legacy physical backup.

- **Use cloud infrastructure services**, which will almost certainly require rethinking how the organization protects infrastructure-as-a-service (IaaS) platforms, as well as adding a software-as-a-service (SaaS)-backup-capable solution for protecting Office 365, Google Apps, or Salesforce (unless the organization already happens to own one of the very few unified backup solutions that protects those SaaS platforms).
- **Build a "private cloud" infrastructure** and **improve collaboration capabilities**, two efforts that also might involve moving to SaaS. And, again, as the organization adds or modernizes those production capabilities, it will have to modernize its protection capabilities as well.

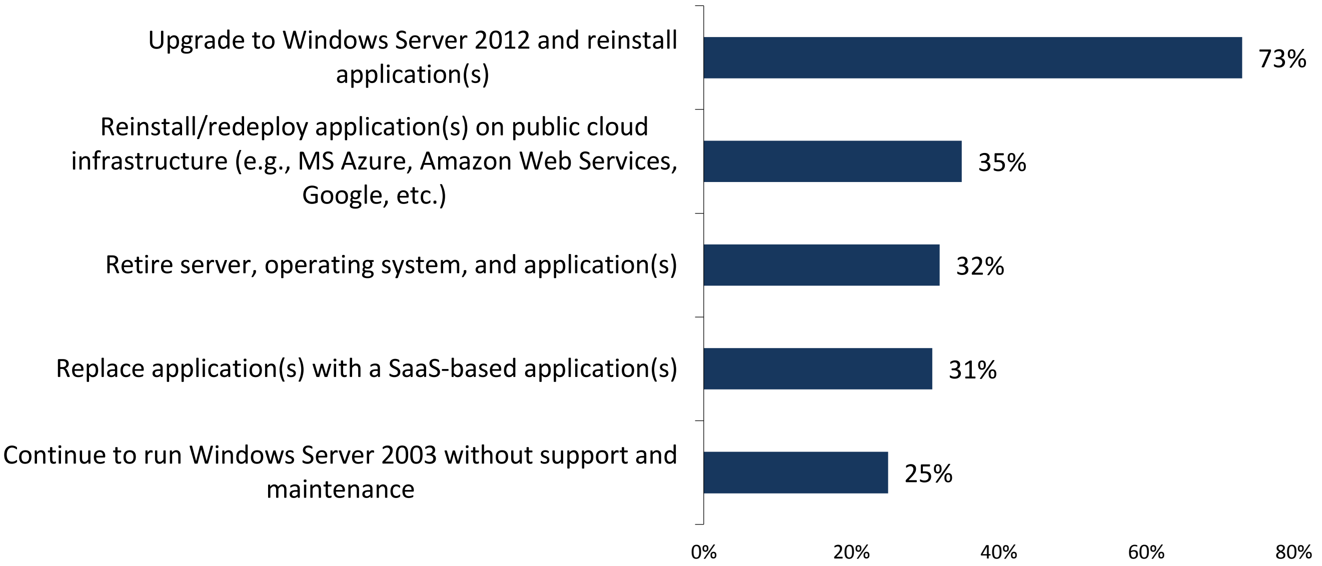
In fact, most IT professionals would probably never modernize their protection capabilities unless some external forcing function was "making" them do so—for example, a production resource is upgraded, and its legacy backup mechanism is now insufficient.

'Good Enough' Is No Longer Good Enough

That reality is especially poignant when considering another data point from the 2015 ESG spending intentions research that depicts organizations' plans for moving off of Windows Server 2003 (see Figure 2).[2]

Figure 2. Plans for Upgrading from and/or Migrating off Windows Server 2003 Systems

What are your organization's plans for upgrading from and/or migrating off of its Windows Server 2003 systems? (Percent of respondents, N=497, multiple responses accepted)



Source: Enterprise Strategy Group, 2015.

Unfortunately, those organizations that are still relying on Windows Server 2003 as a workhorse server platform may also be more likely to be using antiquated data protection mechanisms because WS2003 did not require advanced backup mechanisms and capabilities. To put it another way, the attitude by many seems to be: "*A good-enough production server only warrants a good-enough backup tool.*"

Organizations taking that approach to IT shouldn't be surprised to discover that their backup tool that was barely good enough for Windows Server 2003 is highly unlikely to adequately protect Windows Server 2012, or their VMs (either VMware or Hyper-V), or

ORGANIZATIONS still relying on Windows Server 2003 as a workhorse platform may be more likely to be using antiquated data protection mechanisms. (WS2003 didn't require advanced backup capability.)

[2] ibid.

their SaaS-based platforms such as Office 365. Basically, *none of the platforms shown in Figure 2 are protectable with a legacy approach to backup*.

The Bigger Truth

The example of WS2003 is a timely one, but the broader reality is that most data protection modernization or other IT transformation occurs as a reaction to an outside catalyst. Specifically:

- *Business transformation* is driven by changing user requirements, market conditions, or catalyst events.
- *Production modernization* is (or should be) driven by IT supporting *business transformation* or catalyst events such as a favorite operating system being retired after 12 years.
- *Protection modernization* occurs most often in response to *production modernization* or due to a catalyst event such as a failure to meet SLAs or an inability to reliably restore data.

However the business or IT/production transformation occurs, IT decision makers need to **ask themselves one simple question: "*How are we going to back that up*?"**

If they haven't reassessed that requirement in a while, then IT decision makers are likely to discover that what they have been doing just won't work anymore.