

I D C E X E C U T I V E B R I E F

Building Full IT Infrastructure Protection: How Midsize Firms Can Rise to the Challenge

September 2010

Adapted from [Worldwide Small and Medium-Sized Business 2010–2014 Forecast: Recovery and Change in SMB IT Spending by Category and Region](#) by Ray Boggs, IDC #222409

Sponsored by Symantec

Introduction

Midsize firms are in a challenging position when it comes to implementing, managing, and protecting their IT resources. Firms often have a variety of available technology, usually assembled over a number of years, but the ad hoc nature of many IT environments creates two problems: There may not be a comprehensive vision guiding the coordination and deployment of resources, and just as important, comprehensive protection of those resources may be lacking even as advanced storage and other capabilities are added. This Executive Brief is designed to help technology decision makers look at their technology environments comprehensively to ensure that they are coordinating security and storage resources in a way that provides the optimal coverage necessary to support effective company operations moving forward.

Midsize Firms Are More Squeezed than Anyone

Midsize firms are neither small business start-ups (which typically have fewer than 100 employees) nor large businesses (which typically have 1,000 or more employees). This puts midsize firms in the awkward position of being too sophisticated to have their needs met by the off-the-shelf technology solutions that serve small businesses but lacking the size and scale to justify the kinds of customized, powerful technology resources used by the largest firms.

This is not to say that midsize firms don't have sophisticated technology requirements. These companies are typically advanced in their technology deployments with multiple servers (often dozens), multiple PCs (sometimes in the hundreds), wireless networks, and broadband Internet connectivity. The challenge is that the technology infrastructure has almost always been built up over time and not always with the clarity of vision and purpose that would be considered ideal.

It may come as a surprise to midsize firms, but IDC research indicates that they are actually less efficient in using technology than either small businesses or large businesses, at least when it comes to average IT spending per employee. Small businesses are especially efficient, in part because they underspend on technology and don't have problems like server proliferation and the subsequent need for virtualization that emerge as companies grow. IT staff is still fairly limited in size (usually zero until firms grow beyond 50 employees), and major projects are contracted out rather than handled internally. Large firms are also efficient in that each IT staff member can support an average of 50 or 60 knowledge workers, a higher number than midsize firms average.

While the complexity of large environments can seem daunting, the advanced resources available to manage big company environments help maintain efficiency. Midsize firms simply don't have the ability to leverage their technology management investments to the same degree, which can put them at a competitive disadvantage. The opportunity for better coordination and management of resources is there, but for many midsize firms, daily operational imperatives can delay the real work of improving comprehensive control and protection of existing resources, never mind expanding capabilities by applying new technology.

This brings us to tip number one:

- **Tip #1:** Next to every item on the IT department's "to do" list should be a rating of whether the task advances the larger goal of coordination and full infrastructure protection.

You don't have to focus only on things that advance your long-term objectives, of course, but you should at least be aware of which activities contribute to larger goals and might be worthy of special attention. This additional awareness can improve your progress toward better coordination and alignment of protection performance overall.

Changing Business and IT Spending Priorities — Driving Revenues, Managing Costs Are Key

Small businesses and midsize firms have much in common when it comes to business and IT priorities. Both groups cite growing their revenues as a top business priority in the next 12 months, which is no surprise given the continuing challenge of the economy. But for midsize firms, improving efficiency/productivity is just as important a priority — in a statistical dead heat for first place with growing revenues (see Table 1).

TABLE 1**Top SMB Business Concerns/Priorities for Next 12 Months (% of Respondents)**

Concern/Priority	Small Business	Midsized Business
Grow company revenues	67.6	60.4
Manage costs better	48.1	52.9
Improving efficiency/productivity	45.1	59.0
Add new customers/expand geographically	51.0	47.9
Increase revenues from existing customers	49.7	42.8
Manage cash flow better	48.0	43.7
Identify new partnering opportunities	28.4	28.2
Expand routes to market/distribution channels	21.6	16.2

Note: Multiple responses were allowed.

Source: IDC's U.S. *SMB Survey*, 2010

Midsized firms recognize that while growing revenues is important for long-term success, improving efficiency and productivity can be just as important in enhancing business performance. While smaller firms can tolerate certain inefficiencies as they grow, the same is not true for midsized firms, which need to be attentive to both costs and revenues as key contributors to the bottom line.

Related to the desire for improved worker efficiency and productivity are the IT spending priorities of midsized firms, which are increasingly focused on core infrastructure improvements. Remote worker empowerment is of particular interest to firms, especially those that have trimmed staff in tough times but that are reluctant to return to previous staff levels even as revenue growth has returned. For many companies, the alternative to adding more employees is to increase the productivity of current workers. While this is sometimes seen as "doing more with less," getting more done with fewer employees, it might more appropriately be considered "doing more with more." By providing more resources to remote workers and those at headquarters or branch offices, firms can achieve higher levels of productivity and not have to increase headcount.

One key component of expanding worker productivity through new technology is making sure that critical security capabilities and related infrastructure resources like storage are in place. The

changing role of advanced networks in midsize firms makes higher levels of performance essential. Providing sales staff with real-time inventory information can be a powerful resource to help close a sale during a customer visit. But it also can create vulnerabilities that might lead to unauthorized access of key information.

Similarly, providing account information to remote workers can help them operate with "anytime, anywhere" efficiency, but care must be taken that moves to expanded productivity are matched with equivalent improvements in security protection and disaster recovery to ensure minimal disruption when problems occur.

This brings us to tip number two:

- **Tip #2:** Recognize that the standard 9-to-5 workday is a thing of the past and that there is increasing overlap in personal and business activities 24 x 7.

The same devices used to connect to a company network might be used for personal downloads and access to nonbusiness online resources. This has implications for how you protect your network from threats that might come from internal as well as external sources.

The Challenge of "Complete Protection" and Shift from Point Products to Comprehensive Solutions

The move toward complete protection is one of the most important technology challenges that a midsize company faces. For the smallest businesses, security is at the heart of protection. It might begin with PC connectivity protection — the kind of antivirus, antispam, antispyware, and antispoofing capabilities that help secure PC connections to Internet-based resources. With the addition of local area networks (LANs), especially server-based LANs, the security issues increase in complexity, with both central and endpoint security a concern.

But, as firms grow, other issues emerge beyond just endpoint and network security. Issues of efficiency and effectiveness with regard to data protection become increasingly important. This is where backup and recovery, as well as deduplication and archiving, plays an essential role. Part of this may be driven by regulatory requirements (issues of compliance), but good business practices are the real motivator. The risks of poor performance when it comes to protection are just too great. This brings us to tip number three:

- **Tip #3:** Build your comprehensive protection plan from multiple perspectives — look at where you are now and where you'd like to be, look at network and endpoint activities, and look at where the threats as well as the opportunities for improvement are to be found.

As part of network and endpoint coverage, thinking about internal versus external threats becomes increasingly important. The protection of a secure firewall is essential, of course, but so too is the

internal security of authentication (are you really who you say you are?) and authorization (are you really allowed to see the information you are seeking?). And, of course, beyond those internal basics is the need to make sure that malware is not introduced into the network through USB drives or other unauthorized sources of code that may be inadvertently (or not) connected to the network through mobile devices. The growth in employee use of mobile devices connected to the network has been not only an important contributor to productivity but also a growing complication for company IT departments.

The incentives for comprehensive security protection are both offensive and defensive. On the surface, protections seem almost exclusively defensive — protect what you have rather than help drive revenues forward. In reality, though, effective security is an enabler, much like storage and network capability, that allows a company to move to the next level of resource deployment confident that it is not stepping into harm's way. As firms add the latest advanced mobile communications and computing technology, and expand online resources for both on-premises and remote workers, complete security will be essential.

Comprehensive storage and data protection is also now an important part of a complete security approach. Protecting vital business data is very much a necessity. This is where investment in disaster recovery is critical and where different on-premises and off-premises solutions can be applied. IDC research indicates that firms with 100–499 employees, the heart of the midmarket, do not always back up to remote locations. In fact, 45% indicate that while they do back up regularly, they still keep their data onsite rather than at a separate secure location.

There are three fundamental stakeholders in any comprehensive approach to IT infrastructure protection:

1. **Your own company** that's being protected from potential internal and external threats
2. **Customers and partners** who might suffer harm if their information falls into the wrong hands
3. **The government**

The third is as consequential as the first two, but for different reasons. The government establishes legal compliance requirements and other obligations that will guide the activities of you and all your competitors. The changing regulatory environment makes comprehensive data protection and disaster recovery essential. In some industries like financial services and healthcare, there are strict rules regarding how records are handled. Issues like legal discovery are also influencing data storage and retrieval practices.

Regulations like Sarbanes-Oxley and its equivalents in other countries might seem to influence the actions of only public companies, but even private midsize firms are well advised to establish and maintain compliance. After all, a firm may go public one day or, of more immediate concern, be an acquisition target. Compliance with government reporting guidelines can also be a prerequisite for landing government contracts. In essence, the sooner a firm moves toward regulatory compliance, even if it is not an immediate necessity, the easier that transition will be compared to the future, when a company may be larger and more complex.

New Catalysts for Change — Virtualization, Cloud Computing, and SaaS

The changing nature of technology deployment is posing new challenges for midsize firms even as new opportunities for greater efficiencies and access to more powerful solutions emerge. This brings us to tip number four, and it's a surprising one:

- **Tip #4:** Don't just add more capacity as needs change and protection concerns increase.

While the cost of advanced storage solutions continues to decline, costs like power and cooling, to say nothing about management complexity, can make life more difficult and expensive for IT operations. The growing number of sophisticated workloads can make it tempting to "throw more iron at the problem," but IT professionals are increasingly adopting the following alternative approaches:

- Server virtualization, which keeps physical server counts at manageable levels even as the need for workload-specific servers is addressed
- Cloud computing and software as a service (SaaS), which provide access to advanced capabilities delivered online rather than resident onsite

Server proliferation has not been a problem for small businesses, where the average number of servers continues to be fewer than five. For midsize firms, though, server counts move into the teens and beyond as firms grow. Unlike small businesses, which have continued to add more servers over the past three years, midsize firms have actually had a slight decrease in the average number of servers they use. Virtualization is the answer, of course, with more than half of the midsize firms surveyed indicating that at least one of their physical servers is virtualized. Server virtualization helps with power and cooling costs, of course, but also facilitates effective management as well as the opportunity to expand server resources without new hardware.

Cloud computing is also being deployed with increasing enthusiasm by midsize firms, with roughly 18% of firms having some cloud resources in place and another 18% planning to add cloud capabilities in the next 12 months. In theory, this means that one-third of medium-sized businesses could be relying on cloud computing in the next 12 months.

IDC's definition of cloud computing includes SaaS as well as infrastructure as a service, which would include servers and storage. While the online delivery of software accounts for about three-quarters of cloud computing spending (including SMB spending), the storage and infrastructure parts of cloud computing continue to grow. Online storage is a particularly useful capability, with secure offsite storage part of the value proposition, along with strong disaster recovery capabilities.

Security concerns are cited most often by small businesses as the key factor inhibiting cloud computing adoption. While midsize firms also cite this factor most often, they are far more comfortable with the current status of cloud security. Ultimately, the resources in place to provide secure Internet access will be the same ones providing the protection for cloud resources.

As cloud capabilities increase in importance, the importance of effective security will also increase. The protection of the network firewall will have to be extended virtually to include all the cloud resources that a company uses. This represents a change in the traditional thinking about security, with the need for greater flexibility in management and execution of diverse security solutions.

Integrating the Key Technology Pieces of Security and Storage for Maximum Impact — Next Steps

The convergence of security and storage technology as firms grow is one of the more subtle challenges that midsize firms face. Small firms rely on PC-based storage initially and, as they grow, add server-based storage and network-attached storage (NAS) and perhaps online solutions to take care of backup and data protection. While this may be part of a comprehensive vision of IT infrastructure, it more typically is an ad hoc collection of resources guided by the thinking of multiple IT directors over the years who may have been addressing different corporate objectives.

This brings us to the first step:

- **Step #1:** Look to the past. What IT infrastructure resources have you acquired in different locations, and what has been working effectively? A related question is: How satisfied have different company constituencies (senior management, IT staff, and users) been with IT operations, especially those related to data protection, security, and disaster recovery? This internal audit of resources should yield no surprises but can be an important reminder of where you are starting.

The second step moves from the past (what's in place?) to the present (what are our needs?):

- **Step #2:** Assess the present. Does your company have a growing number of mobile workers that need support? Or does it have new applications that need to be rolled out? These are internal company factors that can influence the pace and direction of infrastructure investment. In a similar way, external factors like regulatory compliance will require continuing attention.

This brings us to the third step:

- **Step # 3:** Look to future needs and prepare accordingly, especially with greater efficiency in mind. Consider the different elements of storage and security that could be coordinated effectively: Disaster recovery, archiving, regular deduping, and virtualization can all play a critical role in improving a company's storage efficiency while improving operational security.

A company's performance needs can vary, of course, but the key is to make sure that your needs have not outstripped your ability to provide effective and timely coverage. Just as important will be the development of a road map of what future performance needs will likely look like so that technology investment can be made with an eye toward addressing tomorrow's needs rather than focusing solely on today's problems.

COPYRIGHT NOTICE

The analyst opinion, analysis, and research results presented in this IDC Executive Brief are drawn directly from the more detailed studies published in IDC Continuous Intelligence Services. Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. Contact IDC Go-to-Market Services at gms@idc.com or the GMS information line at 508-988-7610 to request permission to quote or source IDC or for more information on IDC Executive Briefs. Visit www.idc.com to learn more about IDC subscription and consulting services or www.idc.com/gms to learn more about IDC Go-to-Market Services.

Copyright 2010 IDC. Reproduction is forbidden unless authorized.