IDC
Analyze the Future

WHITE PAPER

Reducing Downtime and Business Loss: Addressing Business Risk with Effective Technology

Sponsored by: HP

Raymond Boggs
Jean S. Bozman
Randy Perry

August 2009

EXECUTIVE SUMMARY

Business risk can appear at your company's doorstep at any time — and in many forms. Systems go offline when aging components fail, natural disasters strike, key networking connections don't work, or a local contractor cuts a power cable. Security issues can emerge and threaten the integrity of business data. All work could come to a halt — or portions of the business could see systems go offline, while others continue to operate normally. No matter the scenario, businesses must plan for such contingencies and what they will do about them when they appear — unbidden — and affect their end users and end customers and their ability to do business.

Maintaining productive and smoothly running business operations is absolutely mission critical — and that is even more evident in today's challenging economic conditions. The critical components of an effective IT infrastructure — servers, storage, software, and all of the networking links — must be up and running, all the time, to maintain business momentum and employee productivity. In many small and even midsize businesses, current IT systems may not be up to date or easy to manage, and this situation sets the stage for potential problems down the road.

Of course, a variety of IT and business challenges are associated with acquiring and maintaining the most effective IT environments to support ongoing operations. Technology must be both affordable and easy to operate on a day-in, day-out basis to effectively support the business. Further, given the business risks of failure, these IT systems must be resilient and flexible, offering the reliability that is essential and the adaptability that will ensure that companies facing growing demands to supply data and services to customers will be able to continue to leverage their IT investments even as their needs change.

IDC customer-based studies show that using appropriate technology in consistent ways helps small and medium-sized (SMB) organizations, even as they address changing requirements. As discussed in the following pages, IDC research with leading SMBs shows that well-targeted technology upgrades, coupled with a rigorous program to standardize and improve IT practices, can deliver substantial risk reduction and could reduce total annual outage risk by as much as 85%, in some cases, with downtime reduced from an average of over 2 hours per month to less than 45 minutes. (The amount of downtime reduction that measures to protect IT infrastructure can deliver represents significant business savings, given that one group of SMBs that IDC studied experienced an average loss of $70,000 per downtime hour.)

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

HP's ProLiant servers can play an important role in supporting business continuity, and serve as a key element of business risk mitigation programs designed to reduce operational costs in today's midsize and large businesses. These x86 servers, which gained a technology refresh with the introduction of the latest generation of ProLiant G6 servers this spring, are widely deployed worldwide. Compared with earlier generations of ProLiant servers, the G6 servers offer faster performance, enhanced management, and dramatically reduced energy costs — and HP is offering new financial terms for purchase or lease to SMBs deploying them. As midsize businesses recognize the escalating importance of their IT infrastructure in reducing business risk and improving business continuity, HP has worked to optimize its technology offerings (servers, storage, and networking equipment) to address their business needs.

Business Risk: What's the Damage?

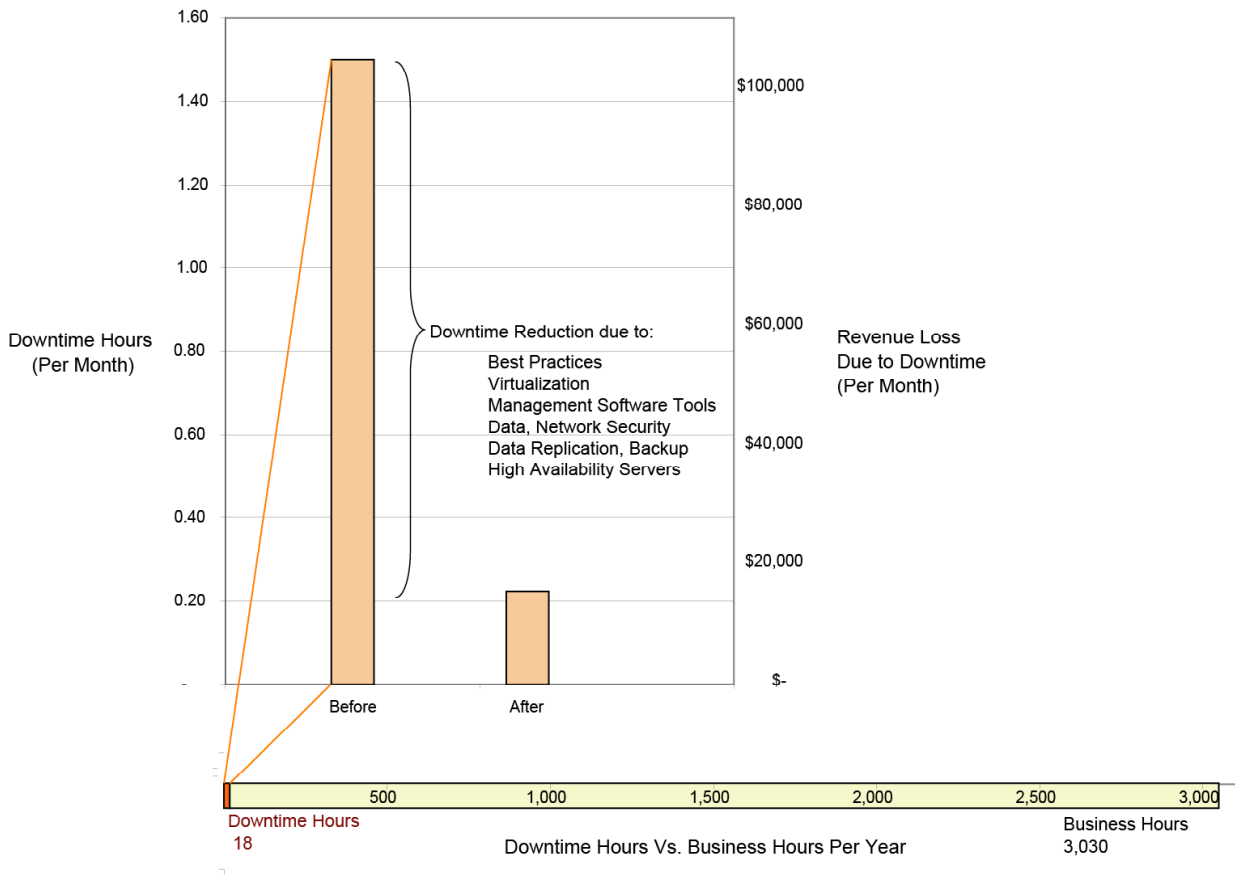
IDC customer-based studies show that each year, the average midsize company experiences 16–20 business hours of network, system, or application downtime. Causes of downtime vary, but aging systems can have components or software that fails, while networking links and power grids can fail at any time because of external causes (e.g., weather, construction work, or natural disaster). Outages occurring during business hours result in revenue loss, as orders are dropped, customers move on, and employees cannot access critical applications. IDC research found that revenue losses per hour averaged $70,000 for one study group.

However, the adoption of best practices has allowed midsize companies to reduce downtime significantly, with an average 25% reduction of downtime annually for the past three years. Solutions that improve system management, protect data assets from loss and unauthorized access, strengthen network security, and ensure availability directly reduce these losses at customer sites. As depicted in Figure 1, IDC ROI research finds that solutions and best practices directed at avoiding such outages — both approaches supported by HP's Business Risk Mitigation solutions — can reduce outages by as much as 85%, cutting downtime per month from over 1.5 hours to less than 15 minutes on average. This means less lost revenue — the actual loss avoided varies from industry to industry, but one IDC study showed average downtime cost at $70,000 per hour. A brief summary of these findings, which show downtime hours per month, and their relationship to revenue loss follows:

- The consistent use of management software tools across the infrastructure reduces network and system downtime by 65%.
- The use of virtualization software reduces server downtime by 10%.
- Adopting industry best practices standards (e.g., ITIL, CobiT) across the organization reduces all downtime by 13% to 15%.

FIGURE 1

The Impact of Downtime on Business and the Value of Reducing It



Note: Revenue loss measures represent an average across many industries, each with differing downtime cost impacts.

Source: IDC's Business Value Research, 2009

Looking at Risk — External Versus Internal

Small businesses (firms with fewer than 100 employees) and midsize firms (those with 100–1,000 employees) face a host of risks, both internal and external. That is, the source of risk can come from outside the company or — perhaps more concerning because it could be prevented — from inside the company.

The external causes of risk are especially challenging — the changing economic environment, new competitors, customers that suffer financial reversals, changing government requirements, and increasing raw material and transportation costs. The one small comfort that a manager can take in these challenges is that they will affect all competitors. No one is immune, although firms can respond to them with different degrees of success.

Easier to anticipate, but no less difficult to address, are the internal risks a company faces. These risks will not adversely affect any company but your own, which makes them all the more important to address. While it may not be possible to prepare adequately for a global economic crisis, it is possible to manage, if not eliminate, the risks associated with internal IT infrastructure problems. These risks fall into three basic categories:

- **System downtime.** When local systems go offline, their data and applications are not available to end users within the organization or to end customers outside the organization who are trying to access data or to buy products/services via a Web interface to the systems/storage/networking components of the IT infrastructure within the company.

- **Network outages.** Loss of network access can halt business operations and in some cases suspend revenue-generating operations. When visible to customers, a suspension of network operations can complicate the delivery of customer service and can even raise questions about a firm's reliability, increasing the opportunity for competitors to take away business.

- **Security breaches.** Even more potentially serious, a security breach can compromise sensitive customer and employee information or intellectual property stored in disk drives or on tape media. Even if data is not corrupted and even if programs are not ruined, the damage to a company's reputation can be catastrophic. Sometimes, news about security breaches surfaces publicly, and the publicity can affect customer loyalty and repeat business by altering customers' perception of the data integrity and data reliability within the organization that experiences the security breach.

While large firms can rely on redundancy and high-availability computing solutions, as implemented by their own IT organizations, many SMB customers must rely on more basic technology approaches that they implement themselves or ask service providers to implement on their behalf. IDC research indicates that SMBs, many of which access central-site infrastructure or third party–operated datacenters, are interested in upgrading their network infrastructure and improving the security of their IT resources (see Table 1).

TABLE 1

Share of Firms Citing Infrastructure as Top Technology Spending Priority (%)

Priority	Small Business	Midsize Business
Increase storage capacity/improve storage management	25.4	30.4
Improve network security/security management	15.9	38.2
Implement/upgrade wireless connectivity	20.0	21.2

Note: Small businesses are firms with fewer than 100 employees, and midsize firms have from 100 to 1,000 employees.

Source: IDC's SMB Survey, 2008

Customer Pain Points

Potential sources for disruption to business processes abound in the modern workplace: Aging systems, inconsistent implementations, and unevenly applied data and security policies all can result in business risk and can threaten business continuity. The top customer pain points include the following:

- **Systems and applications reliability.** Older, less reliable systems cause downtime more frequently than newer systems outfitted with monitoring software that provides alerts to system administrators when a key component fails or goes offline, speeding timely repair. The process of upgrading software or applying security patches can cause system downtime, if not done according to "best practices" that take systems offline for such repair. Virtualization and migration of virtual machines (VMs) to alternate servers during repairs can reduce planned downtime. Physical repairs also need to be made, such as updating aging infrastructure that has too many cables, and too many devices, taped down to furniture, to computer-room posts or ceilings, or under the floor "tiles." Inconsistent backup/recovery procedures mean that some systems are better protected than others; inconsistencies in security and management must be addressed across the entire IT infrastructure.

- **Networking and systems management.** Many SMB organizations lack a single, coherent "view" of systems and networking from a centralized console. This results in an incomplete picture of systems, storage, and networking infrastructure — allowing small problems to develop into big ones before being addressed. In addition, just as SMB organizations have experienced systems sprawl, as many systems were added to the infrastructure in recent years, there has been an accompanying low-end hubs/switch "sprawl," which has grown over the years. Importantly, bandwidth constraints hamper data connections to service partners or to channel partners, who are supporting SMB IT operations, or to central headquarters for a large company that has branch operations across multiple geographic locations. Local sites need high-bandwidth links to stay current with other systems across the network — and to provide local systems with software updates in a timely and efficient way.

- **Security issues across the infrastructure.** For many SMB organizations, the lack of support for single sign-on and authorization across the company prevents accurate approvals for end-user access and could result in inappropriate access to systems by outsiders or hackers. Inconsistent security practices, along with inadequate or aging Internet access methods, leave room for security business risks to develop over time. Data backups that are not regularly scheduled or encrypted can result in security issues related to tampering with data or impacting the integrity of a business' data housed on storage devices or on the organization's PCs. The need to improve employee productivity with wireless networks further increases the risk exposure.

- **PCs and printers at different software release "levels."** The challenge of maintaining aging equipment or updating software for that equipment is widespread in SMB organizations. Inconsistent life-cycle management causes many operational issues. Security lapses associated with data and access to company documents also cause operations issues and unscheduled downtime for end users, affecting their productivity. All of these issues increase IT staff costs, raising operational expenditures (opex) throughout the year.

IDC customer-based studies reveal that IT infrastructure is seen as a top priority in terms of planned spending by companies and their IT organizations. However, in the current economy, many IT organizations are finding that they have to put many of their updating/upgrading/replacement plans on hold, which is impacting planned updates to aging datacenter infrastructure. The importance of keeping IT infrastructure current can be seen in Table 1.

Solutions That Mitigate Business Risk

The adoption of technology solutions can address many of the "specifics" around mitigating business risks, including server refreshes, operating system upgrades, centralized security policies and systems, consistent management practices, storage backup and recovery practices, encryption/deencryption of data files, and networking security for wired and wireless LANs.

Customer "pain points" related to downtime, security issues, or networking issues — or the operational impact of PCs and printers that do not work properly and require repair — are sources of both customer frustration and added cost. Best practices, which are built on solutions already tested to work at customer sites and implemented through management policies, reduce the variations in implementation that often cause business risk to manifest itself in systems that go offline.

HP offers three paths toward providing holistic solutions to address customer pain points relating to business risk: off-the-shelf solutions, channel partner solutions, and HP customizable reference configurations that combine multiple off-the-shelf products into a single solution that can be installed across the organization. All three approaches lead to solutions that can be deployed rapidly and put into use quickly to protect IT infrastructure within the business. We look at each of these approaches in turn in the following sections.

HP Off-the-Shelf-Solutions

HP ProLiant, StorageWorks, ProCurve, Insight Control, PCs, and Printers

HP offers off-the-shelf solutions for business continuity and addressing business risks — such as security solutions, networking solutions, and server/storage solutions. These solutions are based on HP ProLiant G6 servers, HP StorageWorks storage devices, HP ProCurve network switches and wireless network infrastructure, HP Insight Control system management software, and HP Protect Tools for business PCs and HP secure printing, depending on the solution set. The solutions include HP system-level software and software from independent software vendors (ISVs) to

provide all the components of a software "stack" that are needed to complete the solution. These off-the-shelf solutions address customers' needs to reduce IT staff operational costs, including programming and application development costs, as well as troubleshooting costs once the solution is deployed. Examples of these solutions include:

- **Servers.** HP ProLiant G6 servers work with high-availability software that enables a quick restart of applications based on their priority to the business. Software supported includes failover-restart software from a number of software vendors, along with replication software (e.g., HP StorageWorks Storage Mirroring and Marathon Technologies and Neverfail software) that replicates and mirrors data from one site to another. This is useful for planned downtime and high availability, and for disaster recovery purposes, when production data is needed for restarted applications.

- **Virtualization.** Midmarket customers are rapidly discovering that the full savings and availability benefits of virtualization demand highly available storage area networks (SANs). HP enables smaller firms to gain this capability without adding the expense and management complications of external storage networks. The HP Virtualization bundles allow an organization to combine all of the storage that is either inside or directly attached to a ProLiant G6 server into one virtualized pool of storage. Combined with HP ProCurve datacenter networking solutions, this allows an organization to quickly implement a fully virtual infrastructure, with all of its benefits, using pretested building blocks.

- **HP StorageWorks Data Protector Express for automated data backups.** The process of automation reduces pressure on IT staffers to schedule data backup or to conduct the backup process "by hand." Rather, the policies and management of this process are in place and automatically scheduled, ensuring that production data will be ready, when and if needed, for restarted applications.

- **Data security.** HP StorageWorks Data Protector Express' capabilities for encrypting its results prevent intended or unintended snooping; HP's Protect Tools for the client improve PC security and reduce administration overhead to achieve better client security. Extensive wireless security and printing security extensions reduce risk of incursion and malicious access.

- **Security for printing devices.** HP secure printing technologies, including hardware, software, and services, improve the security level for imaging and printing devices deployed in customer sites. This security technology controls end-user access to documents and protects against data tampering with stored, business-critical information.

- **Network security.** HP ProCurve's ProActive Defense networking security solutions provide the midmarket IT shop with switch-integrated security capabilities such as threat detection, virus throttling, and more, which are needed to ensure network uptime continuity and prevent critical data loss.

- **Data backup.** The HP StorageWorks D2D Backup product provides low-bandwidth data replication via disk-to-disk backup, designed to protect data in distributed work environments with multiple servers. Capacity ranges from 1.5TB to 18TB, and the data transfer rate is up to 540GB per hour. The HP D2D systems support HP Dynamic deduplication, which results in more efficient data storage. Deduplication technology reduces the number of copies of data, resulting in a compression in the amount of total storage capacity needed at customer sites.

- **Backup/restore tape devices.** HP also sells the HP StorageWorks LTO-4 Ultrium read/write and WORM drive data cartridges for backup/restore purposes. These cartridges can back up 1GB of data in 8 seconds. The cartridges have 1.6TB of capacity and support data transfer rates up to 240MB per second.

Channel Partner–Led Solutions

HP works with its extensive networks of channel partners worldwide to offer solutions that have been developed and deployed by the channel partners. This approach leverages channel partners' presence in the locations worldwide, using HP products and local channel partner services to complete the specific solution for the customer. With this approach, channel partners add to existing IT staff resources within the customer site and play an active role in assessing specific customer requirements, custom consulting, installing software, deploying systems, and maintaining systems over time. They can also provide ongoing services, including support services and professional services, to maintain, update, or repair the IT solution.

HP Customizable Reference Solutions for Business Risk Mitigation

To address the need for systems that can support key initiatives for business risk mitigation, HP's solution architects review the specific IT requirements for executing a critical business event, such as the implementation of risk mitigation measures or the consolidation of branch offices. In this way, the solution architects develop reference configurations that address customer requirements and enable consistent replication throughout the organization, if needed, to ensure consistent best practice compliance. The implementation then can improve overall reliability across the customer's enterprise or organization.

The primary objective of these reference architectures is to provide affordable infrastructure technology that is easy to adopt and deploy, reducing IT staff costs so that the customer can rapidly put it to work in addressing business requirements. Solution components are selected based upon cost and performance from the broad HP portfolio spanning server, storage, networking, management software, desktop and laptop PCs, and printers/imaging equipment.

ISV Partnerships

HP is also working with a wide array of ISV partners, more than 200 in all, to develop templates that can successfully install applications — and do so in a consistent way that can be easily repeated, thus driving down implementation cost and shortening deployment time. HP worked with VMware to deliver the technology stacks for its HP Virtualization bundles, which are key elements of the business risk mitigation

solution. IDC also notes that one of HP's partners for SMB solutions is Microsoft, which provides Windows-based solutions for SMB companies and branch operations. Finally, HP is leveraging up to 70 "Solution Blocks," which are application-oriented solutions, and working with customers and HP channel partners to install the software, provision new servers, and maintain the solutions over time, reducing ongoing operational costs for IT staff.

HP's Total Care Program

HP's Total Care program is aimed at delivering business benefits over the life of the technology. This is a full-spectrum approach to making IT infrastructure solutions easier to acquire, to deploy, and to maintain over the entire infrastructure life cycle. The ability to replace aging equipment with new equipment — and to do so at reduced acquisition costs — supports customers' programs to reduce business risk for their organizations.

Because technology acquisition is challenging for small and medium-sized businesses in the face of difficult economic conditions, HP is providing new financial offers, including zero percent financing from HP Financial Services, and offering new support/services packages in conjunction with its business partners that provide technical support for new solution deployments:

- **"Recipes" for success.** HP has highly customizable infrastructure solutions that combine server, storage, management, data protection, data security, networking, PCs, and printers. These reference solutions are being provided to customers and HP channel partners to speed deployment of consolidated risk mitigation solutions. Because the components of these solutions have been tested against many operational conditions, they will be easier to support and maintain in the branch office site.

- **Rightsizing of solutions.** HP has designed solutions for businesses of different sizes: those with up to 300 users; 500 users; or 1,000 users. Sizing for the workload is important because it provides the appropriate amount of data processing power, storage, and bandwidth capacity, and it does so for a given number of users to optimize system response time and to boost IT staff and end-user productivity.

- **Ease of use in management tools for system administrators.** IT staff costs must be contained — and the ratio of system administrators to servers and the ratio of administrators to other types of managed devices (e.g., storage, networked PC printers, and networking devices) must be improved wherever possible. Recognizing that system management must be simplified and easy to learn, HP is providing integrated software tools that enable the companies' IT staff and/or their third-party IT service providers to effectively manage the environment from either onsite or offsite (remote) locations.

- **Improved financial terms.** The economic downturn has made it more difficult than before to acquire or lease new technology. HP Financial Services is providing financial terms, including zero percent financing, and improved lease provisions to make it easier to acquire new technology or to refresh technology such as upgrading to the latest generation of ProLiant servers — the G6 servers.

HP Services Addressing Business Risk

- Business operations need to be protected, and repairs or upgrades, if needed, must be handled as quickly and reliably as possible. Midsize companies need to support a range of products — PCs, printers, servers, storage, and software — and they need quick response times to avoid downtime affecting end customers at point-of-sale locations. That is why HP and its channel partners are providing services and support offerings that are tailored to the business needs of SMB organizations seeking to reduce sources of business risk, which drive up operational costs.

- HP and its channel partners offer a range of support services, which can be customized to meet company-specific requirements. HP Care Pack Services provide a portfolio of packaged, affordable, proven services that are scaled to address customer needs throughout the technology life cycle. Two major service offerings for SMB organizations are HP Installation Service, which installs HP-branded products (hardware and software as well as HP-supported products from other vendors), and HP Support Services, which provides integrated hardware and software support services designed specifically for SMB sites' technology.

BUSINESS VALUE RESULTS

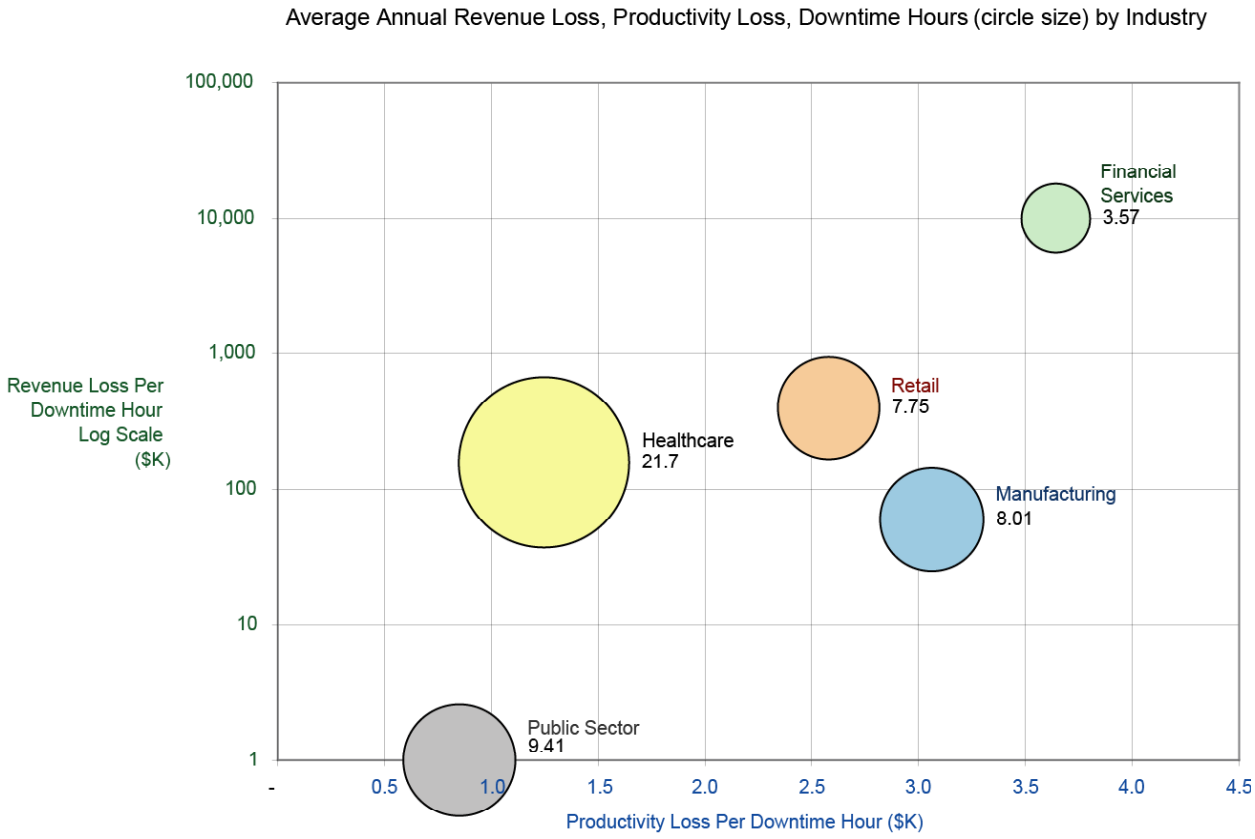
"Before" and "After" Risk Reduction Impacts

To quantify the business risk mitigation value of these types of technology-enabled best practices, IDC used in-depth interviews from multiple surveys of IT practitioners in SMB organizations; these interviews were conducted over the past two years. The makeup of firms that compose the sample set varies in terms of numbers of users, PCs, and servers deployed at the firms' IT sites.

The cost of downtime for midsize companies varies sharply both by industry and by geography. Our research sample covers mostly United States–based companies, so the geographic variations across the regions of the world do not apply to these results. However, the samples showed results that are consistent with the multi-geography studies conducted by IDC from 2006 to 2008. Figure 2 shows the varying cost of an hour of downtime across a selection of industries represented in our 100-firm sample.

FIGURE 2

Revenue Loss, Productivity Loss, and Downtime Hours per Year by Industry



	Productivity Loss / Hour	Revenue Loss / Hour	Downtime Hours
Financial	$3.64	$9,997.50	3.57
Retail	$2.58	$397.50	7.75
Healthcare	$1.25	$157.50	21.70
Manufacturing	$3.06	$59.93	8.01
Public Sector	$0.85	$ .00	9.41

Source: IDC's Business Value Research, 2009

Figure 2 also shows how average downtime hours per year vary by industry. One should notice that cost per hour of downtime inversely relates to the average number of downtime hours per year. IDC notes that this relationship between cost and reported downtime intervals is not coincidental because companies with high-value operations tend to adopt technology initiatives and best practices to reduce risk.

Reducing the Business Risk of Downtime

So which technology initiatives and best practices have the greatest impact on reducing downtime? IDC research about midsize companies has identified the practices and technologies that either have greatly reduced downtime or occur in companies with lower downtime compared with others of similar size, industry, etc. For this white paper, we have selected the technology initiatives and best practices noted in the following list and in Table 2. Each initiative displays the maximum downtime impact holding all other factors constant. These values do not sum to 100 as we measured each initiative's effects on customers' downtime independently.

- Management software tools (65%) to monitor and manage all technology assets include HP products such as HP Insight Control system management software, HP StorageWorks Data Protector Express and HP D2D Backup Systems for automating data protection, ProCurve management for wired and wireless networks, IT service management, information management, application, system and network management, and SOA solutions.

- Server virtualization (10%) reduces downtime arising from system failures and operating system incompatibilities and enhances the ability to shift workloads, further reducing outages by means of planned downtime and migration of virtual machines.

- Enabling failover clustering (43%) for enhancing the availability of internally faced applications.

- Industry best practices processes (e.g., ITIL, CobiT) (13%) make up a set of processes implemented uniformly across the entire organization to centrally manage all aspects of IT.

- Thin clients/blades (25% PC downtime) reduce hardware failures caused by user errors, software incompatibilities, or physical damage and theft.

- Comprehensive PC security (28% PC downtime) is a set of technologies that reduce PC vulnerability to external security threats. All notebooks and desktops are equipped with encryption, access control, antivirus utilities, antispyware/malware utilities, centrally managed PC firewalls, and an automated patch distribution system that supports software updates and patching while reducing demands on IT staff time.

- Standardizing on one desktop operating system, version, and release level (30%).

- Upgrading servers, storage, and networking hardware (50%) sustains more advanced, faster versions of these hardware devices and reduces risks of downtime caused by aged or out-of-synch platforms.

- Deploying antivirus and antispam solutions throughout the organization (15%).

TABLE 2

Downtime Reductions Enabled by Specific Initiatives (%)

Initiative	Downtime Reduction
Management tools	65
Upgrade servers, storage, networking	50
Failover clustering for internally faced applications	43
Standardization on single desktop operating system	30
Comprehensive PC security	28
Thin clients/blades	25
Deploying multiple antivirus, antispam solutions	15
Industry best practices implementation (ITIL, CobiT, etc.)	13
Server virtualization	10

Notes:
Percentages do not add to 100.
Effects were measured independent of each other.

Source: IDC's Business Value Research, 2009

CHALLENGES/OPPORTUNITIES

Business risks take many forms — including risks to IT infrastructure encompassing servers, storage and networking equipment, and endpoint devices such as PCs and printers. Security threats impact customers' data and cause networking downtime. This in turn delays or prevents the communication of voice and data inside and outside the company. It impacts customers and business partners. Current economic conditions are highlighting the need to avoid business risks because any interruption to business processes will result in lost revenue and increased costs due to damage control potential impacts on customer retention.

HP is well-positioned to address these business risks because of its deep and broad inventory of hardware, software, and services that enable companies to keep watch over the "state" of their systems, storage, and networking equipment; PCs; and printers. These technologies, combined with management/monitoring software, allow business customers to respond to threats of disruption effectively and affordably.

CONCLUSION

Downtime and security threats cannot be prevented, but they can be isolated by taking a holistic approach to identifying business risks and to addressing each of the major causes of business risk. The value proposition associated with HP solutions for business risk mitigation is that business risks can be mitigated by leveraging actual customer experiences to develop "best practices" that deal with the actual causes of business risk, thus reducing the operational costs incurred by disruptions and recoveries. Customers can accelerate their "learning curve" around these best practices by using services that build on proven reference architectures and by refreshing technology through updates to servers, storage, networking hardware, high-availability software, virtualization, data replication software, and data security and management software, as needed, to improve reliability, availability, and security.

This combination, leveraging updated technology and best practices together, has been shown to reduce costs associated with downtime by 30% to 60% and to reduce the amount of lost productivity by up to 80%. Further gains can be made: By adopting best practices and updating IT infrastructure, companies can lower annual downtime by up to 85%, greatly reducing interruptions to daily data processing and access, supporting business continuity, and containing operational costs.