

White paper

10 Strategies to Optimize IT Spending in an Economic Downturn

January 2009

**Tim Clark, Partner
The FactPoint Group
300 Third Street, Suite 10
Los Altos, CA 94022, USA
1 (650) 233 1748
tclark@factpoint.com**

Today's IT environment

“Basically you’ve had to throw away any plan you’ve put together prior to the end of August [2008] and start over again.”

—*Peter Whatnell, CIO, Sunoco. (Wall Street Journal, Dec. 8, 2008)*

In the economic downturn, IT budgets are shrinking even as expectations of how technology can help the business are growing. To benefit their companies, IT managers optimize operations, cut costs, anticipate and address problems before they happen, and resolve issues quickly when things go wrong. That means streamlining operations and actively managing their computing infrastructure.

In other words, back to basics, such as:

Assure security. All the advanced capabilities that IT can enable don't count for much without protection. Network security represents “table stakes” to get into the game. Nobody wants to take a chance on whether the enterprise is secure.

Be proactive. Plan for cuts—or for more cuts—before they are mandated. Assemble a cost-cutting team now. Structure cutbacks in stages so if the economy continues to decline, your company is ready for additional reductions.

Work smarter: The traditional IT approach has been to hold off on hardware purchases. Instead, build new capabilities for the recovery. Walk away from legacy applications that cost too much to support, Gartner suggests, arguing that tough times call for politically touchy changes. Turn off idle equipment to save utility costs. Consolidate data centers (HP has gone from 85 to 6.).

Redeploy IT resources: Prioritize revenue-producing initiatives. For instance, new business intelligence implementations can help analyze new market segments or prioritize internal budget cuts.

Reduce complexity: Many organizations are virtualizing infrastructure—servers, storage, even desktops—to simplify IT management. However, others, especially mid-market companies, remain unconvinced of virtualization's virtues.

Strive for agility: Expect consolidation among your customers. A customer involved in a merger may combine operations, and that can produce fast-closing sales opportunities. IT must support the business in making fast transitions.

Top 10 strategies to optimize IT spending in tough times

1. Numbers talk, so use them

Financial justification of all things IT becomes vitally important in a down economy. Return on investment (ROI), reduced total cost of ownership (TCO) and quick payback periods on technology purchases become even stronger factors. IT buyers may also re-evaluate their preferences for top-tier brands such as Cisco or IBM, or at least ask whether they're worth the premium pricing.

Numbers count not only in acquiring new hardware and software but also in justifying ongoing IT operations. Reporting is critical, and clear, graphical presentation of the figures can impress the number-crunchers.

2. Use hardware appliances

Hardware appliances are dedicated devices that run a specific application. By running an application on an appliance, IT departments reduce their management burden since appliances are usually "plug and play" and include their own infrastructure stack. Appliances also can be more secure because they run on stripped-down operating systems. Some appliance vendors will manage the appliance for customers or give them a management interface to administer multiple appliances on their network.

Akin to hardware appliances are virtual or software appliances, self-contained applications that run as virtual machines in a virtual environment, often VMware. Software appliances are appropriate for many business applications, but not necessarily for security applications.

3. Use multi-function devices

Similar in concept to hardware appliances are multi-function devices that run two or more related applications on a single dedicated device. Multi-function devices address the problem of a proliferation of hardware appliances in an enterprise. Appliances have their merits, but hosting them for multiple applications can quickly cause an overpopulation in the data center.

To reduce management overhead and cut utility costs, consider the versatility of hardware such as Unified Threat Management (UTM) devices. A UTM device puts multiple security applications—such as a subset of antivirus, anti-spam, firewall, virtual private network (VPN), intrusion prevention, anti-malware, application firewall and content filtering—on a single dedicated hardware appliance. In March 2008, market researcher IDC reported that UTM devices are even replacing routers in the low-end market, and IDC expects further consolidation in the low-end segment.

Multi-function devices are common for security applications and, they are gaining popularity in areas such as systems management and network applications.

4. Telework

Companies are beginning to see telecommuting as an opportunity, not an issue. In an April 2008 survey by WorldatWork, 42% of U.S. companies had telework programs, up from 30% in 2007. In Canada, the figure jumped from 25% in 2007 to 40% in 2008.

Gartner tips on IT savings

Gartner, the IT analyst firm, offers its list of suggestions to save IT money in the downturn:

Review invoices to be sure you're paying only what's in the contract.

Stop paying for unused software. Harvest unused licenses for new employees.

Ask the CFO to scrutinize the IT budget—she/he can align IT with the big picture.

Thin middle management in IT to flatten the organization

Defer moving to Vista for a year.

Reduce storage costs with deduplication.

Cut tolerances on availability: Settle for 3 nines when you don't need 5 nines. Each "9" adds 30% to the budget, Gartner says.

Use the Internet instead of pricey WAN transport services when possible.

Business benefits from telecommuting and "green" considerations drive that growth. Start with higher-quality new hires and better retention rates. Sun Microsystems says its telecommuters cite its telework program as the No. 1 reason they would recommend Sun.

In a June 2008 survey by job recruiter Dice, 37% of IT workers say they'd accept up to a 10% lower salary to work full-time from home. Better retention a clear boost to the IT budget because it holds down the cost of recruiting and training new hires. More telecommuters also mean savings for the company on IT, facilities and utility overhead and can boost employee productivity.

However, telework may add burdens on IT. The most obvious requirement is secure remote access to keep data safe between the home office and the corporate office. Web conferencing helps keep telecommuters in touch with the rest of the organization and reduces the need for business travel, particularly for sales and marketing staff. Companies might also explore Voice over IP (VoIP) for teleworkers to help cap phone costs.

5. Automate endpoint control

With more remote users, including teleworkers, companies need a policy-driven system to handle access to resources on the corporate network. For starters, set a policy that requires access devices have the latest versions of security, antivirus and anti-spam software to keep malware off the corporate network.

Then automate enforcement of the policy with technology that insists endpoints are adequately protected before they're allowed to connect. The enforcement software must permit fine-grained authentication of users and assess the security level of the device and its location. Once the security policy is set, let the technology enforce it.

6. Reduce the number of IT suppliers

One source of IT complexity and cost is supporting hardware and software from different vendors. Too often IT departments devote internal or outside resources just to make incompatible devices or applications work together.

The first line of IT defence is to purchase products that support industry standards. But advanced features result from extending the standards, making desirable functionality incompatible with other IT operations.

The next option is to standardize on a limited number of vendors, who are generally good about making their new gear work with their old gear, to reduce integration headaches. After a merger or acquisition, enterprises often have multiple applications for the same function. Eliminate duplicate applications to reduce licensing and support costs. In consolidating vendors, especially when demand is slowing, negotiate hard and don't be afraid to switch. Question sticking with the status quo.

7. Look at hosted offerings

Cash constraints make hosted (or service-based) offerings more compelling. Unlike traditional on-premise applications, Software as a Service (SaaS) and managed services generally don't require big upfront license fees. When cash is tight, that's an advantage. IT should see SaaS as reducing its workload, not as a threat.

A related move is toward shared services, such as a single help desk. Accomplish that either by consolidating existing internal help desks (for different divisions or for recent acquisitions) or by outsourcing that function to an external service provider.

8. Shift storage and processing to the cloud.

Cloud computing is topical, and one aspect is that enterprises can outsource storage or heavy-duty processing to service providers in "the cloud." Common applications that enterprises are currently sending to the cloud fall in three categories:

- Those that require periodic but heavy demand on compute resources—end-of-month closing for accounting apps or heavy seasonal demand before the holiday for e-tailers.
- High-performance computing (HPC) applications that require lots of heavy duty computation such as drug discovery for pharmaceuticals.
- Disaster recovery, when enterprises need back-up capacity in case a primary data center goes down.

The big boys—Amazon S3/EC2, Google, Microsoft Azure—grab most of the media hype, but they're not the only players. Many local and regional computer resellers have cloud offerings too, sometimes specialized on applications such as business continuity. With Amazon cutting prices on S3 in October 2008, look for increasingly competitive pricing.

9. Explore Web 2.0 apps

Look to consumer applications and Web 2.0 technologies to enhance productivity and improve outreach. Your employees use these applications at home or on their portable devices, so they're familiar and require little training. They allow employees to do at work what they can do at home. IT departments would do well to consider consumer-oriented Web 2.0 technologies for interfaces on their proprietary internal applications.

Because they're consumer-focused, Web 2.0 technologies are often cheap and sometimes free. Marketing departments are increasingly using Web 2.0 applications to help retain clients and reach new customers, mission-critical activities in a downturn. IT should be ready to handle Web 2.0 applications soon, if not already.

10. Boost productivity

In a world that demands doing more with less, IT must empower workers with more effective productivity tools. Spiffy new applications are one way, but Gartner suggests training for business users on existing software tools may help too. It's cheaper than writing new code, and many users utilize only a small fraction of any application's capabilities. In other words, they already have more power and more productivity at their fingertips, so teach them to take advantage.

Conclusion: Security in the downturn

Beyond the specific actions outlined above, no IT department can afford to compromise on security in a downturn or any other time. Without protection, the rest of IT's many capabilities won't matter much.

Many of the strategies outlined in this white paper will challenge the traditional network security model, which must stretch to accommodate telecommuting, cloud computing, SaaS, Web 2.0 and managed services. It's time to adjust how security is provided.

A new security model is emerging to account for these trends and accommodate securing the distributed nature of organizations of all sizes. The problem is described by the term "de-perimeterization," a way of saying that security perimeters, once the moat that protected enterprises by keeping the bad guys out, don't matter much anymore.

Remote sites, customer sites and outsourcing partners all lay outside the traditional security perimeter as do mobile and wireless devices and WiFi-equipped laptops. These all create new opportunities for security breaches. To protect all these elements, as well as the core network and data centers themselves, requires multiple layers of defense or a "defence in depth" security model. The result: Secure access to resources by users and endpoint devices beyond the perimeter plus secure data traffic crossing the perimeter.

Some of the new Web 2.0 applications also devour bandwidth, putting them in competition with mission-critical applications. IT must be able to prioritize usage of network bandwidth based on the application, file type or user profile.

For example, peer-to-peer applications carry little or no benefit to an enterprise but they can consume critical bandwidth. IT must bar peer-to-peer applications or pinch them with bandwidth limits. In a tough economy, buying more corporate bandwidth for your YouTube users is not high on the corporate priority list.

How SonicWALL® fits in a strategy to cap IT spend

SonicWALL® markets two classes of products that are relevant to IT departments looking to save money and benefit the business during the economic downturn. Its Unified Threat Management (UTM) line of network security appliances bundle firewalls with security subscriptions such as anti-virus, intrusion prevention and anti-spyware. SonicWALL also offers secure remote access SSL VPN (virtual private network) devices for remote workers connecting to corporate networks.

How does SonicWALL fit in a strategy to optimize IT spending in the downturn?

Most critically, SonicWALL's Clean VPN strategy enables organizations to deliver:

- **Secure Access** to designated network resources for a broad array of users, including mobile and fixed endpoints, remote offices, contractors and business partners. That secure access means an enterprise to do business beyond the security perimeter.
- **Multi-Threat** or Threat-Free **Protection** from the uninspected content—potentially viruses, spam or other malware—that will flow through any SSL VPN access. That ensures both in-bound protection from malware and out-bound protection from the loss of corporate data.

Beyond the Clean VPN security model, SonicWALL security products also address other strategies outlined in this white paper. SonicWALL products are available on multi-function hardware appliances. With SonicWALL's next-generation network security appliance, companies can consolidate security applications running on separate pieces of hardware onto a single piece of multi-function hardware for easier, cheaper management and lower power consumption. With SonicWALL UTM devices, multiple security applications can be updated with a single download instead of separate ones for each application.

Another recent feature on SonicWALL's next-generation network security appliance is Application Firewall, which can prioritize bandwidth usage by user profile, application or file type. Application Firewall dramatically increases employee productivity and gives priority to mission-critical applications that drive revenue.

Telecommuters and other remote users can gain secure access to corporate resources using Aventail Secure Remote Access SSL VPN and SonicWALL SSL VPN, thus increasing productivity of remote users. The same products can assure secure access to employees of newly acquired companies who may work in separate locations.

For the IT helpdesk, SonicWALL's Virtual Assist allows sharing the desktop of any remote machine, reducing the time and cost of support calls, both remote and within the same building.

SonicWALL's Global Management Service (GMS) provides a single console for remote management of SonicWALL appliances as well as some devices from other vendors. GMS reduces the need for an extended IT workforce by making existing personnel more efficient. GMS' strong reporting features can be spiffed up with SonicWALL add-on product ViewPoint for compelling reports and documenting compliance requirements.

SonicWALL Email Security stops all spam and other email threats at the gateway, increasing employee productivity. The solution's ease of use requires minimal IT support, from installation to every-day management.

Visit the SonicWALL web site at www.sonicwall.com for more information on SonicWALL Network Security Solutions.

About SonicWALL

SonicWALL is committed to improving the performance and productivity of businesses of all sizes by engineering the cost and complexity out of running a secure network. For more information, visit the company Web site at <http://www.sonicwall.com/>. Secure remote access information is available at http://www.sonicwall.com/us/products/Secure_Remote_Access.html.

About The FactPoint Group

The FactPoint Group (www.factpoint.com) is a Silicon Valley-based market research, publishing and consulting firm specializing in the early adoption of new technologies. The FactPoint Group has been producing world class research, analysis, and consulting since 1993 and continues to help its clients sell and use new technology solutions. FactPoint partner Tim Clark previously was a senior editor with CNET News.com, where he covered Internet security.