

An Ounce of Prevention: The IT Imperative for Small and Midsized Businesses

EXECUTIVE SUMMARY

For businesses of all sizes and industries, IT and network management are more challenging—and important—than ever before. Large organizations have long understood the advantages of outsourcing IT and network support. Now many small and midsized businesses (SMBs) are recognizing the strategic and economic advantages of managed services.

In this paper, Ricoh explores some of the drivers behind managed services and then outlines an approach that SMBs can use to begin the journey to managing technology with greater effectiveness, security and cost-efficiency.



UNDERSTANDING THE CHALLENGES

Few business owners and executives need to be convinced that IT and network management are challenging endeavors—particularly when an organization lacks dedicated internal IT resources. Almost every business' operations depend upon reliable, secure network access to complete a range of processes—from fulfilling orders, managing accounts receivable and payable and, in many cases, delivering services to customers. Indeed, anyone who has experienced a network outage knows how painful (and costly) such incidents can be. At the same time, end users everywhere need someone to help them overcome software and hardware issues when they arise.

An Ounce of Prevention: The IT Imperative for Small and Midsized Businesses

ARTICLE HIGHLIGHTS NETWORK SECURITY RISKS FOR SMBs

"Hackers Shift Attacks to Small Firms," *The Wall Street Journal* reported in July 2011. In the front-page article, the *Journal* shared the story of a small-business owner in Chicago who had been a hacking victim:

"Recent hacking attacks on Sony Corp. and Lockheed Martin Corp. grabbed headlines. What happened at City Newsstand Inc. last year did not.

"Unbeknownst to owner Joe Angelastri, cyber thieves planted a software program on the cash registers at his two Chicago-area magazine shops that sent customer credit-card numbers to Russia. MasterCard Inc. demanded an investigation, at Mr. Angelastri's expense, and the whole ordeal left him out about \$22,000."

The article goes on to note that hackers are no longer focusing their efforts solely on large, multinational corporations. Instead, they are going after any business that stores data in electronic form. And they have discovered that small businesses are often easy targets.

In fact, the *Wall Street Journal* cited statistics from Verizon and the US Secret Service that in 2009, just 27 percent of cyber attacks targeted companies with 100 or fewer users. In 2010, 63 percent of such attacks were on small businesses.

Industry research suggests that SMB owners fully understand the challenges, but still lack viable solutions. For example, the *Symantec 2010 SMB Information Protection Survey* of small (10 to 99 employees) and midsized businesses (100 to 499 employees) confirmed that security is an important concern: "When asked to rank various business threats, SMBs placed data loss and cyber attacks as their top two risks, eclipsing traditional criminal activity, natural disasters and terrorism.

"Furthermore, they rated computer security, backup-recovery and archiving and disaster preparedness as the top areas they planned to improve over the next 12 months. These were rated higher than traditional IT improvement areas, such as improving computing performance, increasing data storage capacity or even reducing computing costs."

Despite this awareness—and fear of threats to security, many SMBs are still relying on a patchwork of reactive support for their networks and IT environments. They assume that they are protected until it is too late. That creates vulnerabilities that can be exploited by hackers or even disgruntled employees. And that can result in significant costs—or even the closure of a business.

Indeed, a more recent study, *Symantec 2011 SMB Disaster Preparedness Survey*, reports that SMBs experienced a median of six outages in the past year. The report goes on to note that downtime costs SMBs a median of \$12,500. "It costs small businesses a median of \$3,000 per day and medium businesses a median of \$23,000 per day," the report notes.



An Ounce of Prevention:

The IT Imperative for Small and Midsized Businesses

“By taking a more proactive approach to IT and network management, organizations can avoid problems before they occur.”

REGULAR CHECKUPS

Getting a physical examination from the doctor provides a valuable snapshot of an individual’s health. But real results are achieved through ongoing and proactive maintenance of health and wellness.

The same holds true for any network. While a Teknoforce Proactive Health Check provides an invaluable baseline measurement for network performance and security, organizations will achieve better results with ongoing maintenance, management and support.

In fact, after an organization signs on for Ricoh managed services, it will be able to see, at any time of the day or night, the health of its network on an individualized website. In addition, Ricoh reviews these results in formal monthly “checkups” with the client for the first 90 days and quarterly reviews thereafter.

RECOGNIZING THE OPPORTUNITIES

Large organizations have long relied on advanced technologies for remote management and support to streamline and automate key network maintenance and security functions. Historically, these have been cost prohibitive for SMBs. But SMBs are now recognizing—and tapping into—the advantages of these remote managed services through third-party providers.

Arguably the most important benefits come down to **prevention** and **predictability**. By taking a more proactive approach to IT and network management, organizations can avoid problems before they occur. That translates to more predictable network performance and more predictable technology costs.

Of course, a proactive approach to network management offers other benefits, as well. Such benefits include:

- Increased employee efficiency, since workers are able to do their jobs with few or no “fires” to fight
- Enhanced network performance, as patches, antivirus updates, backups and security activities are seamlessly automated
- Better assurance for business continuity because events are proactively identified—and resolved—before they affect day-to-day operations

The bottom line: When it comes to IT and network management, the old adage about an “ounce of prevention” holds true.

A PRUDENT FIRST STEP: ASSESSING THE CURRENT SITUATION

Many SMBs remain oblivious to the state of their network and the pervasive threats that may have already penetrated it. Those that are aware of the risks recognize the potential advantages of managed services for proactive network management and support. But they may find it difficult to take that first step toward engaging a provider—or they may procrastinate, thinking (and hoping) that a major network outage or security breach simply will not happen within their organization.

An Ounce of Prevention: The IT Imperative for Small and Midsized Businesses

REVIEWS COVER THE FOLLOWING AREAS:

- *Patch management.* Patching is essential in the effort to prevent viruses, spyware and malware from infiltrating a network. In addition, some compliance requirements—including PCI, HIPAA and CIPA—mandate that organizations perform patch management.
- *Antivirus software.* Ricoh assumes responsibility for maintaining, monitoring and remediating antivirus software.
- *Event logs.* Ricoh proactively identifies errors that have occurred on servers since installation and then performs associated fixes.
- *Alarm notifications.* Ricoh prepares a list of alarms generated and explains associated risks—illuminating the productivity that would have been lost if systems were down.
- *Backup and disaster recovery (optional).* Ricoh's service may also include ongoing backups, as well as assurance that backups have been successfully completed.

A simple, low-risk first step is **Ricoh's Teknoforce Proactive Health Check**. With this assessment, Ricoh installs a software program, called a probe, on a company's devices running on the network. Devices may include PCs and servers, as well as tablets, smartphones and other mobile devices. With the probe in place, Ricoh monitors them for several days. Based on that real-world activity, Ricoh prepares an executive summary that helps an organization understand its network's strengths and weaknesses. More specifically, the Teknoforce Proactive Health Check can reveal that:

- *A network is at risk.* Microsoft® Windows® environments require regular patching. Without such maintenance, malware circulating the Internet can exploit vulnerabilities in Windows—causing poor performance or downtime or even compromising confidential information.
- *Software licenses are not compliant.* Microsoft and other software providers may audit an organization for license compliance. If a company is out of compliance, it could face stiff financial penalties. Ricoh's Teknoforce Proactive Health Check is able to identify where multiple software licenses from most software vendors exist in a network—making it easier to identify and remediate any licensing issues.
- *Data is in peril.* When a server hard drive is nearly full—but no one realizes it—some programs will simply stop working. Such programs could include email, a mission-critical application for almost all businesses.

Ultimately, Ricoh provides an Executive Summary and report card scoring individual items and the overall network on a scale of 0% (lowest) to 100% (highest). The overview includes:

- All system activity, identifying devices with failed backups and hardware and/or software changes
- A server update, identifying the number of times servers have failed
- Operating systems and disk space used, listing the operating systems' platforms and the amount of unused disk space, enabling businesses to right-size devices
- Patch status, detailing the number of patches installed, missing, denied, pending and failed.

Most SMBs find the results of their Teknoforce Proactive Health Check—which show gaps in security and performance—to be eye-opening and motivational. What's more, if an organization decides to invest in managed services from Ricoh, the Health Check results provide a benchmark that can be used to monitor and track the performance improvements that Ricoh delivers.

An Ounce of Prevention:

The IT Imperative for Small and Midsized Businesses

THE NUTS AND BOLTS: HOW DOES A TEKNOFORCE PROACTIVE HEALTH CHECK WORK?

Ricoh's Teknoforce Proactive Health Check is accomplished with software agents developed by Kaseya, the leader in IT services monitoring and optimization technology, under the technical specifications listed to the right.



Ricoh's Teknoforce Proactive Health Check is a simple first step to what can become a smart and effective approach to IT and network management. With a suite of managed IT services, SMBs enjoy end-to-end, enterprise-level support from certified professionals—including remediation, proactive monitoring and maintenance, helpdesk support and on-site service as needed.

1. Ricoh uses the 5721 TCP outbound port for the communication with the Kaseya agent. Since the agent initiates the communication from *inside* the firewall, no security holes are made in the existing network protection.
2. The size of the executable to install the agent is approximately 2 megabytes (prior to installation). While running, the agent size is approximately 16 megabytes. (The agent must be installed with local administrator credentials.) Because it does not take up a lot of system capacity, end users should not experience any noticeable impacts on performance.
3. Once installed, the agent is fully self-sufficient. It runs as a service with local system credentials (that is, no admin credentials are required by user-run scripts), and any actions—such as system patches and scans—can be completed without user intervention.
4. All data sent between the agent and the hosted servers are encrypted with a rolling RC4 encryption key. Thus, even if data were somehow captured, it would be meaningless without the encryption key.
5. Once installed, the agent will inventory all hardware, executable and license keys from the machine where the agent has been installed. This information is sent over the encrypted tunnel to the hosted server and stored in a Microsoft® SQL Server® database.
6. We then query the SQL database to run reports on the environment. The data stored in the SQL database is text representative of the hardware, software, performance statistics and license keys installed on a system with the monitoring agent. No data is removed from any hard drives; we do not send actual files to the data center from the machine with the agent installed.
7. Ricoh's hosted environment is an ISO 27001-certified data center with multi-tiered redundancies for power, network and hardware. There is also a secondary environment, which can be turned on in the event of a site failure. The backup site offers full redundancy and security.
8. When checking in to the server, the agent sends approximately one 90KB packet per minute. The size of data transfer will increase if there are actions pending for the agent to complete. Examples include executing a script or reporting the results of a system scan (similar to the one that occurs upon installation of the agent).

An Ounce of Prevention: The IT Imperative for Small and Midsized Businesses

MINIMUM SYSTEM REQUIREMENTS FOR TEKNOFORCE PROACTIVE SERVICES

To effectively monitor and manage an SMB's environment, its network must be brought up to date and must meet the following system requirements:

- Workstation OS is Windows XP, Windows Vista or Windows 7
- Server OS is a version of Server 2003 or Server 2008
- CPU of 2 GHZ or better
- Memory of 1 GB or better
- Customer will have an enterprise-class firewall from SonicWall, Cisco, Fortinet, WatchGuard or Juniper

If an organization does not meet these criteria, Ricoh can assist in updating the environment to achieve maximum performance and security and to enjoy the full benefits of Ricoh's Teknoforce Proactive Services

LOOKING AHEAD

For virtually any small or midsized business, and especially for those moving to the cloud, network performance and security is becoming more—not less—important. SMBs are also going to face ever-greater threats in the form of viruses, spyware and other security breaches.

With that in mind, SMBs are wise to explore the options for a more disciplined, strategic and predictable approach to managing their IT infrastructure—and particularly the network backbone.



FOR SMBs, THE FUTURE COULD BE IN THE CLOUD

Many SMBs are taking a closer look at how cloud-based services can free them from having to invest in expensive IT infrastructure and related ongoing maintenance. In addition to IT network services, some companies are adopting cloud solutions for document management, email, collaboration and customer relationship management.

However, relying on cloud-based solutions raises a number of important issues that need careful consideration, such as access, security and reliability. These concerns mean SMBs should move judiciously when placing business-critical services in the cloud. A recent survey by Symantec validates those concerns—showing the “big gap between expectations and actual results” among those who had implemented cloud technologiesⁱⁱⁱ

An Ounce of Prevention: The IT Imperative for Small and Midsized Businesses

“Using a Software-as-a-Service (SaaS) platform for document storage and management frees a business from the time and expense associated with physical document storage.”

One cloud solution that has received wide acceptance among SMBs is document storage and back-up. A recent study by IT trade association, CompTIA found that an overwhelming 71 percent of the SMBs surveyed had some form of cloud-based service for these document management functions.^{iv}

The popularity of cloud storage and back-up among SMBs is not hard to understand. Using a Software as a Service (SaaS) platform for document storage and management frees a business from the time and expense associated with physical document storage. It also reduces the risk of potential loss or business interruption possible with on-site storage of paper-based documents due to a disaster, such as a fire, flood or criminal activity. Another likely reason that cloud-based document management is growing in popularity with SMBs is that it ties in directly with another important trend: mobile communications. Smartphones and tablets are rapidly changing not only the way businesses interact with customers, but also how employees communicate and engage in their work. Among small businesses, the CompTIA survey found that 25 percent were actively using mobile solutions and an additional 43 percent expected to within 12 months. A cloud-based document management system complements this trend, giving employees access to critical documents no matter where they are working.

For a minimum additional monthly fee, Ricoh’s Teknoforce Proactive Services can include both on-premises and cloud back-up and disaster recovery services, with full redundancy, through our two data centers.

i. http://www.symantec.com/content/en/us/about/media/pdfs/symc_2011_SMB_DP_Survey_Report_Global.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jan_worldwide_dpssurvey

ii. http://www.symantec.com/content/en/us/about/media/pdfs/symc_2011_SMB_DP_Survey_Report_Global.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jan_worldwide_dpssurvey

iii. <http://www.reuters.com/article/2011/10/04/us-computing-cloud-survey-idUSTRE7932G720111004>

iv. http://www.comptia.org/news/pressreleases/11-07-27/Technology_Enabling_SMBs_to_Become_More_Mobile_and_Competitive_New_CompTIA_Study_Finds.aspx

ABOUT RICOH TEKNOFORCE IT SERVICES

Ricoh Teknoforce delivers expert technical assistance and network support with nationwide coverage for any size organization in any industry. Ricoh offers a single source for all IT service needs, whether an organization is building a network from scratch or seeking to improve IT performance. Ultimately, Ricoh enables organizations to offload time-consuming tasks, ensure high network uptime and security, and take a more proactive approach to upgrades, maintenance and issue resolution.

Teknoforce support services include:

- **Proactive Services.** From Ricoh's state-of-the-art Managed Services Operations Center (MSOC), Ricoh Teknoforce Proactive Services help improve network performance and reduce the risk of outages that can compromise a business. Maintenance and monitoring processes help ensure peak performance of an IT infrastructure (servers and workstations) 24/7, and increase employee efficiency. If Ricoh detects suspicious activity, we can either notify an organization's IT team to solve the problem or resolve it remotely.
- **Responsive Support.** With more than 2,220 certified technicians nationwide, Ricoh Teknoforce's on-demand IT support enables an organization to supplement the capacity of its IT department. It also allows smaller businesses to acquire professional IT skills and services without making a considerable investment in human resources.
- **Voice Over IP Integration.** Ricoh Teknoforce can connect your phone, desktop and organizational communications into a single, easy-to-use interface—which employees can access via desktop and mobile phone.
- **Network and Data Security.** Ricoh offers solutions to help secure networks, including firewall installation and maintenance, and partnering with SonicWall to support disaster recovery and a variety of Continuous Data Protection (CDP) solutions. Further, Ricoh Teknoforce Proactive Services defend servers and PCs with anti-virus and anti-malware, and guard data both locally and in a secure off-site location.
- **Large Enterprise Solutions.** Ricoh Network Support Services, staffed by over 2,200 expert IT engineers, offers a unique, cost-effective solution for large organizations. With our combination of national coverage, proven IT services expertise, and portfolio of remote and on-site services, we can help you add IT capacity on short notice, outsource time-consuming, non-critical tasks, and maintain a higher level of consistency across the enterprise.
- **Leasing.** With continuous pressure to control costs and do more with less, it is often difficult to acquire the necessary services and equipment to run a business within budgetary constraints. Leasing IT hardware offers the flexibility to minimize risk, maximize productivity and preserve initial capital investment for use in higher-return investments.

The content of this document, and the appearance, features and specifications of Ricoh products and services are subject to change from time to time without notice. While care has been taken to ensure the accuracy of this information, Ricoh makes no representations or warranties about the accuracy, completeness or adequacy of the information contained herein, and shall not be liable for any errors or omissions in these materials. The only warranties for Ricoh products and services are as set forth in the express warranty statements accompanying them. Nothing herein shall be construed as constituting an additional warranty. Your actual results, including print speed and other performance measures, will vary depending upon your use of the products and services, and the conditions and factors affecting performance. THERE ARE NO GUARANTEES THAT YOU WILL ACHIEVE RESULTS SIMILAR TO OURS. RICOH DOES NOT WARRANT THAT OUR PRODUCTS OR SERVICES WILL GUARANTEE OR ENSURE COMPLIANCE WITH ANY LAW, REGULATION OR SIMILAR REQUIREMENT.

© 2012 Ricoh Americas Corporation. All rights reserved. Company names, product names and trademarks mentioned within this document are the property and trademarks of their respective owners.

RICOH® and the Ricoh logo are registered trademarks of Ricoh Company, Ltd.

The RICOH logo is displayed in a bold, red, sans-serif font. The letters are closely spaced and have a slight shadow effect, giving it a three-dimensional appearance. The logo is positioned in the bottom right corner of the page.