WHITE PAPER

Communication, Collaboration and Content Management Best Practices for Small Businesses

An Osterman Research White Paper

Published August 2011

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

Executive Summary

ABOUT THIS WHITE PAPER

This white paper offers succinct advice to small businesses in the areas of communication, collaboration and content management technology. Its purpose is to educate the small business owner and IT director about the best practices in these areas, and to highlight a range of newer developments that offer significant benefits to small businesses. It is sponsored by Cleartext, McAfee and Safend. Information on the relevant offerings from each of these companies is provided at the end of this white paper.

KEY TAKEAWAYS

Key takeaways from the white paper are:

- Small businesses face many of the same challenges as their larger enterprise counterparts in managing communications and other systems, but they also suffer from additional issues. In a highly competitive market, this can count against the small business in significant ways.

- Small businesses should not necessarily eliminate smaller vendors from consideration in their email, social media, instant messaging and other communication and collaboration system planning. While large vendors should, of course, be considered, so should smaller vendors.

- Unified communications services deliver flexibility benefits to end-users by bringing together various communication tools in a holistic package. The infrastructure is simplified too, as a consequence of removing multiple single-purpose tools in preference to a multi-purpose infrastructure.

- Also important in the context of unification is the ability to deploy new collaboration and communication technologies that include integrated security and compliance capabilities. Using such integrated systems will reduce the cost of managing the IT infrastructure and will ensure more cohesive management of the infrastructure.

- Small businesses should not rely on public Internet services for real-time business collaboration, but should deploy business-grade capabilities or acquire them through a business-class cloud provider. There are significant business benefits to be gained by switching to real-time collaboration, but these can be lost by inappropriate reliance on public services.

- Many organizations have developed robust security, policy and management capabilities for email, and need to apply the same level of rigor to their instant messaging, microblogging and social media capabilities. A failure to apply the same consideration to real-time communications as to email can expose an organization to significant security and other risks. Many organizations have done an adequate job at protecting their email-related threats, but may still have holes in their security and compliance policies for non-email communications.

- Capturing and retaining content and communication transmitted through a range of services for long periods of time is essential to small businesses – this includes email, social media,

microblogging, instant messaging and any other system that manages business records. While there are legal and regulatory reasons for doing so, it also makes good business sense to know what is being promised to clients, prospects, and business partners by retaining and appropriately managing long-term access to these records.

- Cloud providers offer a range of content technologies that enable small businesses to be flexible, nimble, and up-to-date with effective and efficient ways of working. While the on-premise deployment model continues to be viable, gone are the days when deploying capabilities on-premises is the only way to go.

- Being a small business is no excuse for taking a lax stance toward security, whether for on-premise deployments or cloud-based services. Common security approaches, such as anti-virus protection, anti-spam filtering and anti-malware are critical for businesses of all sizes. Again, these need to be applied to instant messaging, microblogging and social media as they are to email.

- With the rise of cloud-based providers, every small business needs to consider its strategy for on-premises versus cloud-based service delivery. Striking a balance between the two approaches is essential, although given the fundamental economics of the cloud-based approach, it is likely that small businesses will make greater use of cloud services in the years to come.

The Traditional and Unique Problems Faced by Small Businesses

SMALL BUSINESSES FACE THE SAME PROBLEMS AS ENTERPRISES

Small businesses, generally classified as those with fewer than 500 employees, face many of the same problems as their larger enterprise counterparts. The world has shrunk, adding pressure from new domestic and international competitors to firms of all sizes, not just the gargantuan enterprise with fingers in every market. In responding to this pressure, businesses across the size spectrum need to make informed decisions about resource allocation and use IT to keep abreast of the moves and countermoves of a growing array of competitors.

The same applies to keeping up with government regulations and legal requirements in multiple markets. Both large and small firms face budget constraints, especially in these times of economic uncertainty, hardship and austerity. What's true for one is true for the other, and there are devastating flow-on effects to small businesses when large businesses retrench their outsourcing activities. Finally, whether employees work for large or small firms, the increased use of mobile devices – such as smartphones and tablets – adds complexity to the challenge of IT management, and introduces a whole raft of practical considerations that need careful consideration.

SMALL BUSINESSES HAVE FEWER CRITICAL RESOURCES

However, while common issues abound, small businesses face challenges their large counterparts do not:

- Very small businesses normally lack dedicated IT staff, and typically must rely instead on external consultants to address issues as they arise – in many instances, systems are too complex to be deployed, configured and managed by internal staff that are not trained and experienced in key technologies.

- Businesses in the range of 50 to 300 employees typically have dedicated IT staff, but these staff members are, of necessity, IT generalists rather than dedicated specialists.

- Larger businesses (i.e., those with more than 300 employees) normally can afford to have IT specialists on staff.

Where small businesses lack dedicated IT staff members, it is typically for ongoing server maintenance and common administration tasks, but also for the more complex tasks of deploying new technologies to improve business operations. Being a small business means that total IT costs can be spread only over a small number of employees, leading to higher costs on a per-employee basis. The economies of scale for IT spending enjoyed by enterprises are not experienced by small businesses, making them more sensitive to IT investments, and less likely to invest in the infrastructure they need to be competitive.

SMALL BUSINESSES PAY MUCH MORE FOR IT ON A PER-SEAT BASIS

To illustrate the degree to which small businesses pay a much greater cost for IT infrastructure on a per-seat basis, we have outlined the costs of deploying and managing Microsoft Exchange for a 10-, 100- and 1,000-user environment, as shown in the following table.

Three-Year Costs of Ownership for On-Premise Microsoft Exchange

HARDWARE	10 Users	100 Users	1,000 Users
E-mail server	$2,378	$2,378	$9,512
Three-year 24x7 support, four-hour response	$2,199	$2,199	$8,796
AV/AS appliance	$1,698	$3,397	$4,397
SOFTWARE	**10 Users**	**100 Users**	**1,000 Users**
Server software	$699	$699	$15,996
Client access licenses	$670	$6,700	$67,000
Software maintenance	$1,050	$10,500	$105,000
Windows Server 2008	$3,699	$3,699	$14,796
Addl. server OS software client access licenses or equivalent	$0	$2,996	$38,951
Clients	$1,000	$10,000	$100,000
LABOR	**10 Users**	**100 Users**	**1,000 Users**
IT admin cost (Year 1)	$32,000	$32,000	$160,000
IT admin cost (Year 2)	$33,600	$33,600	$168,000
IT admin cost (Year 3)	$35,280	$35,280	$176,400
TOTAL THREE-YEAR TOTAL COST OF OWNERSHIP	**$114,273**	**$143,448**	**$868,848**
TOTAL THREE-YEAR TCO PER USER	**$11,427**	**$1,434.48**	**$868.85**
TOTAL ANNUAL COST PER USER	**$3,809**	**$478.16**	**$289.62**
TOTAL MONTHLY COST PER USER	**$317.43**	**$39.85**	**$24.13**

As but one example of the cost penalty that small businesses incur simply by virtue of their small size is the cost of Windows Server 2008. As shown in the table, a single copy of this server software will suffice for both the 10- and 100-user deployment, but the smaller business will pay 10 times the cost for this server software on a per-user basis.

Best Practices for Communication

EMAIL IS NOT THE ONLY COMMUNICATION TOOL

Despite the rise of many new forms of communication technology during the past several years, email continues to be a key method for communicating in a work context. It's the vehicle through which many people work – goals are shared, tasks are allocated, and conversations are negotiated. If we add the capability for sending files to others, email is also the predominant way of routing work among staff. For example, an Osterman Research survey conducted in late 2010 found that the typical user sends 43 emails on a typical workday and receives 123 – an average of one email sent or received every 2.9 minutes during a typical eight-hour workday. Further, the typical user spends a mean of 134 minutes per day using email, more than the telephone, instant messaging and social media combined.

Clearly, email is critical and it's unlikely that it will be wholly replaced in most organizations. This is not meant to imply that other forms of communication are not also important, but email will continue to lead the communications focus in many small businesses for some time.

THERE ARE MANY SMALLER VENDORS THAT CAN MEET SMALL BUSINESSES' EMAIL REQUIREMENTS

While certain large vendors have a stranglehold on the email server market for enterprise customers, small businesses have more flexibility to choose a product that's fit-to-purpose for their requirements. There are many smaller vendors that can meet the email requirements of small businesses. The products from these vendors offer many benefits: lower licensing costs in comparison to those charged by the large vendors, less investment required for IT consultants to install and maintain email services, and greater flexibility in integrating with user-facing and backend infrastructure, such as office productivity suites for users and directory and collaboration servers on the backend. Indeed, small vendors focus on the best overall email experience, and less on locking the customer to their array of complementary products. Moving away from the email products from large vendors creates more room for flexibility across the entire IT portfolio and there is little risk in doing so.

WHY SMALL BUSINESSES SHOULD CONSIDER MIGRATION TO UNIFIED COMMUNICATIONS

One technology advance that small businesses should consider is unified communications. With unified communications, different communication tools – such as email, voicemail, and real-time communications like telephony and instant messaging – are brought together in a unified package. This can improve communication because staff can see their conversation and interaction history with clients, prospects, and coworkers in a single unified place. They no longer have to manually keep track of what was said to whom on what date through different communication tools – unified communications automatically brings it all together.

For small businesses, this unification offers the potential of lower cost of ownership, because multiple single-purpose communication infrastructures give way to a single, multi-purpose one. As well as eliminating the need for users to switch between different tools, thereby simplifying both training programs and everyday communication tasks, it also takes away the need to pay external consultants to keep a disparate set of infrastructures running.

Finally, unified communications greatly simplifies life for mobile workers, because all of their communication activities are controllable through a single interface. Email and voice mail are presented together in a unified inbox, accessible from any device – thereby immediately getting rid of the need to call the office and navigate the voicemail system. Initiating communication is also simplified, particularly if real-time interactions are offered with presence-aware indicators. This means that mobile workers can see if their co-workers are available for discussion, even when neither party is in the office – streamlining the resolution of critical issues and ensuring a continual focus on delivering what the client needs.

Effective tools for communication are essential for small businesses, and there is a range of innovations available that increase capability, streamline operations, and eliminate costly duplication of resources.

Best Practices for Collaboration

MOST SMALL BUSINESSES RELY ON PUBLIC TOOLS FOR REAL-TIME COLLABORATION

The rise of a new generation of collaboration tools on the public Internet has re-contoured the way we keep in touch with our friends and family. Twitter enables us to share what we're thinking as it happens – no more email newsletters at the end of the month. Facebook gives grandma a new way of seeing what her grandchildren are up to, and for people to share and comment on personal and work activities. Instant messaging and presence services like AOL Instant Messenger and Skype provide the capability for having extended private chats by text, video or voice. These are great tools for use in private life, but their crossover into the realm of business communication is troublesome.

Small businesses should not rely on public Internet services for real-time collaboration, but should instead make use of business-grade services. Securing content and making it available only to authorized parties is essential in a business context, and public services can't deliver the assurance required that this is happening. In a similar vein, the archival of real-time collaboration transcripts from business conversations and activities is essential, and "best effort" attempts are not enough. When significant business decisions are being discussed using collaboration services, having the guarantee that unauthorized parties aren't eavesdropping is more than a nice-to-have – it's essential. Finally, keeping internal systems free from virus attacks and malware is a never-ending battle, but using public services for real-time collaboration is akin to throwing open the door and welcoming attacks with open arms. In summary, a business-grade service is required for instant messaging, social media and microblogging – something that's built for business and fit-to-purpose.

THE BENEFITS OF REAL-TIME COLLABORATION

Real-time collaboration services offer many benefits to small businesses. In these highly competitive times, where a delay in making a decision can result in profitable work going to a competitor, having the ability to quickly bring together the decision makers, wherever they happen to be located due to travel commitments, can be a competitive differentiator. You can discuss the parameters of the decision by voice, allowing a much richer interaction than anything email messages can afford – and it's dealt with immediately as well, not two or three days later when everyone gets around to clearing their email. Equally, documents and presentations can be co-developed without being in the same office, allowing a speed-of-response and depth of analysis that traditionally don't go together.

Working together through real-time collaboration services also benefits small businesses by increasing efficiency compared to email traffic. We have already touched on the effect of shrinking elapsed time by dealing with issues via real-time collaboration rather than email messages, but efficiency benefits can be gained in other ways, as well. Conversations between three or more people are hard to follow in email threads, largely because people respond to different parts of the thread, resulting in confusion. It takes more time to unpick what someone was trying to say across an email thread compared to hearing it live within the context of a spoken discussion. Moreover, when documents are being routed back-and-forth for comment and review, confusion is compounded and version control problems can further slow decision-making. For those who are trying to clear their email backlog, the chances are they will rush the job and pay less attention to the details of the communication, making a mere "best efforts" attempt to respond to what they thought the other person was trying to say. Collaboration via email can work, but it's very inefficient compared to newer ways of working together via real-time collaboration services.

Connecting employees using real-time collaboration services offers the flexibility for remote working. Employees don't have to visit the office merely to be seen or to take part in critical conversations – they can do that from wherever they are. They can perform effective work wherever they need to be, based on client requirements and their own lifestyle choices. This flexibility has the flow-on effect of reducing employee turnover and therefore eliminates additional recruiting costs, because less enlightened but perhaps larger enterprises are less able to put a more attractive job proposition on the table.

Finally, real-time collaboration creates the opportunity for reducing real estate costs and associated taxes and other costs. There was a time when having an address in a particular location was important to winning new business and exhibiting an aura of success, but that's less so now. Employees with the capability to perform great work wherever they are, and also to stay in touch with their coworkers without being forced to visit the office, reduce the need for pricey real estate.

In summary, new forms of real-time collaboration offer significant benefits to small businesses.

Best Practices for Content Management

SMALL BUSINESSES MUST ARCHIVE ALL RELEVANT CONTENT

Keeping good records about what has been promised to clients and business partners is merely good business practice. The opposite – being blind to what has been promised – is fraught with significant business risks and legal exposure. For this reason, small businesses must archive all relevant content, and with the proliferation of tools used by employees for communication and collaboration, that's a significant task. In addition to archiving, however – that being the capture of the content transaction – is the need for proactive alerts on key phrases, along with random sampling to gauge the level of risk for the organization.

Archiving vendors offer the most mature tools for capturing and storing electronic communication. Real-time conversations also need to be captured, however, by regulation for firms in the financial services sector, and by good business practice for anyone else if the tool is being used for business communication. Instant messaging conversations, BlackBerry PIN messaging, microblogging and even social media activity status updates must all be considered under a holistic approach to content management in small businesses. Overall, the basic principle is that any electronic content that might be required for legal, regulatory or other purposes should be captured and managed appropriately.

In jurisdictions that legislate in a way that requires email archiving, the relevant law often talks about electronic communication (or Electronically Stored Information [ESI]). This means that archiving and e-discovery solutions deployed for email need to be replicated within an organization's instant messaging, social media and microblogging platforms in the same manner as they are for email. Increasingly, courts and regulators draw little distinction between ESI in an email and ESI in any other electronic record, such as an instant message, tweet or Facebook post.

OTHER TECHNOLOGIES THAT ANY SMALL BUSINESS SHOULD CONSIDER

A number of other content technologies are available that make sense for small businesses, given their unique challenges around being effective with IT in the face of practical and financial restrictions:

- **Cloud-based storage**
  Instead of creating a backup infrastructure onsite and ensuring that tapes are correctly rotated on a daily and weekly basis, cloud-based storage synchronizes internal systems with a secure backup location in the cloud. As data inside the organization changes, it is securely backed up. If a disaster strikes – which has become more top-of-mind due to the earthquakes, tsunamis, and tornados in 2011 – a business can keep operating even if they have to rapidly evacuate their primary premises.

  Cloud-based storage for content synchronization is a related example of a content technology that's appropriate for small businesses. Many small businesses are giving up on the capital costs and operating headaches of having a file server onsite, and are instead embracing synchronized cloud storage. This means that employees can access their working files wherever they are, using a variety of devices—including smartphones and tablets. Employees can also work collaboratively with coworkers and clients by having secure access to the same data and documents, and can eliminate the hassles of email and

file attachments. Changes made on any device are synchronized back to the cloud, enabling everyone to have streamlined access to the latest version, wherever they are.

- **Managed file transfer**
  A managed file-transfer solution is the third example of a content technology that small businesses should consider. Large files clog email networks, are often rejected at the firewall, and run the risk of being intercepted when sent over regular email. With a managed file-transfer solution, greater reliability is guaranteed for both sender and recipient. The sender uploads their file to a secure location and then passes a unique Web address to the recipient. When the recipient, or recipients in the situation of a multi-party collaboration, accesses the file with a user name and password, the solution creates an audit history of access and downloads. Such an audit trail provides vital records to protect a business from charges of breach of contract, among other things.

- **Electronic signature capabilities**
  Electronic signature services also offer value for small businesses, eliminating the need for a fax machine and poorly reproduced copies of contracts and other vital business records. When a signature is required, the contract is uploaded to the secure electronic signature service, the target areas for signatures identified on the document, and the names of the people to sign the document linked with each area. The service then contacts each person individually and requests his or her review of and signature for the document. No paper is generated through the entire process, ensuring a streamlined workflow and the elimination of accidental loss of critical in-progress documents.

- **Proof-of-delivery technologies**
  Finally, content proof-of-delivery technologies ensure small businesses gain the legal proof needed for messages and documents transmitted by email, and save significant costs over alternatives such as FedEx. The proof is admissible for legal matters, and this gives peace-of-mind for messages and documents that absolutely have to get through and be proven to have gotten through. Often the alternative is an expensive overnight parcel delivery with a signature required, but with content proof-of-delivery it just happens as part of a regular email flow.

Managing content is a must for small businesses, and there are a range of approaches and technologies that will streamline and simplify the content management challenges of such firms.

Best Practices for Security

SECURITY NEEDS TO BE A CENTRAL ISSUE IN EVERY DEPLOYMENT DECISION

Security is a core issue for all types of communication, collaboration and content management applications, and being a small business is no excuse for taking a lax attitude on this front. There are many different security approaches available for small businesses, and we will look at five main systems in this section.

KEY SECURITY CAPABILITIES THAT MUST BE DEPLOYED

There are three critical security capabilities that every small business should deploy: anti-virus, anti-spam, and anti-malware:

- Anti-virus protection ensures that viruses embedded in email messages, attachments distributed by real-time communication services, and files accessible through a Web browser are stopped before they wreak havoc. While protecting internal systems is vital, it's even more important to ensure that your customers are not adversely affected by your own lack of anti-virus protection. This war can be won only by everyone doing their part – becoming known as the company that distributed a virus to its customers is highly detrimental to future business prospects.

- Anti-spam capabilities tend to block unwanted email messages, some marketing campaigns, and the offer of great riches from widows of former world leaders. Unwanted messages are extraneous to standard business communication and clutter email inboxes and email servers, and will consume the vast majority of an organization's Internet bandwidth if preventative measures are not taken. Aside from the financial costs associated with not filtering for spam, represented by additional Internet bandwidth cost and extra servers to handle the growth in email traffic, is the productivity drain inflicted on end users in dealing with a torrent of spam. With the competitive dynamics we touched on earlier, small businesses can't afford to pay employees to manually sort unwanted spam from real email messages. Anti-spam technologies have become even more critical because of the increasing use of blended threats – spam messages that contain a link to a malware-laden site that can infect a computer with malware.

- Anti-malware security systems prevent malicious code embedded in software programs from causing a system meltdown. Malware attacks may delete critical system files on desktop and laptop computers, thereby crippling the very tools that end users work with on a moment-by-moment basis. Or they can intercept passwords for critical systems, including the business bank account, and send details to a third party. Suddenly running out of cash due to theft is an anathema to being productive, and by the time you have recouped the loss, your business may have suffered irreparable damage and loss of trade. There are numerous examples of small businesses that have been infected with the Zeus bot, for example, resulting in the loss of tens or hundreds of thousands of dollars within a few minutes' time.

DLP AND CONTENT PROTECTION ARE CRITICAL

Two additional security offerings are worthy of particular attention by small businesses. Preventing the distribution of confidential business content is the focus of content inspection and filtering tools – commonly known as data leak protection (DLP). These capabilities will ensure protection for content distributed by email, through Web 2.0 applications, and for data that is held on removable media such as thumb drives or is synchronized to a smartphone or tablet.

In the case of email messages, DLP software will prevent unauthorized recipients from reading attached files. Because a large proportion of the sensitive content that leaves an organization is in attachments – e.g., word processing documents that contain Social Security numbers, customer financial information or employee healthcare records; spreadsheets that contain

sensitive financial information; and other content that users create as a normal part of their work – the use of DLP for email is critical. Organizations that do not employ DLP run the risk of violating data breach notification laws, losing trade secrets or suffering other serious consequences.

For data and documents held on removable media, DLP will ensure that the correct user is accessing the material and, if not, will prevent access. And, for smartphones or tablets that fall into the wrong hands, remote wipe capabilities ensure that while the device may be compromised, the data never will be.

NON-EMAIL CHANNELS ARE EQUALLY IMPORTANT TO PROTECT

While there is not a significant amount of spam in non-email communication channels, any content control or DLP rules that an organization has deployed for their email content must be duplicated in their instant messaging, social media and microblogging solutions to ensure matching levels of security and legal protection. For example, there is a significant threat from URLs passed through Twitter in the context of introducing malware into an organization through phishing – the application of URL filtering and other Web security technologies must be applied to less traditional ingress points, as well as to traditional ones like email.

CONTENT ENCRYPTION IS ALSO VITAL

The final area of security that small businesses should pay attention to is content encryption for hard drives, removable storage devices and outbound content. Any employee who carries a business laptop or tablet with them should be encrypting the storage on the device, so that if the device is lost or stolen the data will not be compromised. For example, losing internal data like trade secrets can have major implications on new product development efforts and overall competitiveness. Worse, if confidential data is stolen and posted to a public Web site, there are scenarios in which a company can actually lose its ownership of those trade secrets. Moreover, even small businesses must comply with data breach notification laws – the costs to remediate even a single data breach can be in the hundreds of thousands of dollars and could potentially bankrupt a small business.

Modern operating systems for businesses include encryption capabilities out-of-the-box, and various providers offer add-on services to enhance these base capabilities. Anyone still using Windows XP, or an organization without a Windows 7 site license, may want to consider the use of third party encryption software or Self Encrypting Drives. Removable storage devices, such as thumb drives, are a common way of transporting files between locations. Organizations that do not want the data distributed across the Internet or sold to their main competitor should take action and make sure their removable storage devices are encrypted. Organizations can use hardware-encrypted devices, or better yet, employ software encryption for the USB devices they already own. Finally, outbound content carrying important business information should also be encrypted to prevent inadvertent or malicious access by unauthorized parties.

Any small business should develop policies for protecting content. These should include employee-focused policies that spell out the need to use encryption on any company-owned or personal smartphone, laptop, flash drive, tablet, desktop computer, CD, DVD, etc.; and the requirement to send confidential information in a secure manner when it is transmitted via email, file transfer systems, instant messaging systems, via social media or physically. Further, policies should be implemented that will discuss how sensitive and confidential information

needs to be encrypted when stored on file servers, FTP systems, collaboration databases, document management systems, etc. These policies should clearly lay out the consequences of violating corporate encryption policies and the use of personal devices for work-related applications, particularly when used to send, receive or store sensitive information.

Security is important. Without it, a small business opens itself to significant technical and business risks, and failing to take adequate measures can be the kiss of death – it can literally put a company out of business.

Key Decision Points for the Cloud

THE CLOUD IS WELL SUITED TO THE NEEDS OF SMALL BUSINESSES

The rise of cloud-based services for communication, collaboration and content management is very promising for small businesses. With a pay-as-you-go pricing strategy and few structural barriers to swapping cloud providers, small businesses gain tremendous flexibility to optimize their IT spend and gain access to capabilities that were traditionally reserved for their much larger enterprise counterparts. What used to require months of planning and the deployment of significant infrastructure elements, can now be had within minutes with the flash of a credit card. In a world of heightened competition, the cloud is a great equalizer for small businesses.

SECURITY IN THE CLOUD

One of the primary areas in which the cloud can be used very effectively for small businesses (and for very large ones, as well) is for anti-virus, anti-spam and anti-malware protection. By modifying MX records so that incoming email is routed through a cloud provider for filtering, small businesses can eliminate virtually all of the unwanted and dangerous content from their incoming email stream without the requirement for any on-premise infrastructure. This can dramatically reduce the cost of email security and provide protection on par with that of the largest organizations.

Moreover, cloud-based security can also be employed in a number of other areas, as well, including encryption of outbound content, archiving, DLP for email and other communication tools and other capabilities.

HOWEVER, ON-PREMISE SYSTEMS CAN ALSO BE HIGHLY EFFECTIVE IN A SMALL BUSINESS ENVIRONMENT

While cloud-based providers offer tremendous benefits for small businesses, there is still a place for on-premises systems. Small businesses with a preference for higher initial capital costs and lower ongoing operational expenses – in contrast to the month-by-month operational expenses of cloud services – will find a range of on-premises systems that can deliver the benefits discussed in this white paper. In the same way, small businesses that predominately operate out of a single location are likely to experience faster system performance for employees from on-premises systems, compared to cloud-based services that must be accessed through an external Internet connection. When the majority of traffic can stay inside the building, the promise of cloud-power diminishes.

A third factor when considering the difference between cloud and on-premises delivery is short-term flexibility. Businesses that need short-term access to computing power – in the range of a

couple of days to a week – can leverage the instantly available offerings in the cloud. When the computing requirement has been met, it's just a cost to expense, rather than a fixed asset to liquidate. If the need is more constant and a particular computing resource can be purchased to deliver the requirement more cost-effectively than a cloud-based service, on-premises infrastructure could be the way to proceed.

STRIKING A BALANCE BETWEEN THE CLOUD AND ON-PREMISE

Nevertheless, it's not an either-or proposition, and every small business should complete a due diligence exercise on what's available from cloud providers. There are capabilities available at an attractive price point that might make a hybrid IT strategy more appropriate than 100% on-premise or 100% cloud. There is a middle ground to be explored between the two delivery options. For example, small businesses with a single location will gain benefits from the strategic use of cloud services to complement a predominantly on-premises strategy. One example is the use of cloud-based backup and recovery services in order to back up content to a geographic location far from the corporate location in the event of a natural disaster.

As another example, small businesses that require specialized services on an infrequent basis are better served through the cloud – think managed file-transfer, electronic signatures, and content proof-of-delivery services, for example. With the possibility of service delivery through the cloud, small businesses can up-level their IT capabilities for only infrequent applications, rather than having to go without altogether and taking the perception hit with customers and prospects. Of course, any due diligence exercise on cloud offerings will have to be renewed at least every six months, given the frequency with which new offerings are being introduced.

Both on-premises and cloud-based service delivery modes will improve in the coming years, although it is highly likely that the rate of innovation with cloud-based services will outstrip the on-premises model. It's fundamentally easier to add new capabilities to a small number of data centers and radiate those capabilities out to customers, compared to delivering updated software for download and installation by IT consultants. Small businesses need to consider their approach to IT given the longer-term trajectory of both delivery models.

Regardless of the specific choice for the in-the-cloud versus on-premises debate, having the discussion internally is vital, if for nothing else than to mitigate the risk that you have overlooked a new source of competitive advantage.

Questions to Ask

There are a number of questions that any small business' decision makers should ask about their capabilities and best practices, including:

- How much do our email system, collaboration systems, content management systems, security and other IT infrastructure cost us when considering the total cost of ownership, including labor, opportunity costs and licensing?

- Do we evaluate new on-premises and cloud-based vendors with enough regularity to understand their offerings?

- Have we considered how we can make best use of unified communications?
- Are we using business-grade communication and collaboration services where it is appropriate to do so, or are we relying too heavily on "public" services?
- Are we archiving content in accordance with our regulatory, legal and best practice requirements?
- Are we backing up our data appropriately for purposes of disaster recovery and business continuity?
- Are we using managed file transfer capabilities and/or services where it makes sense to do so?
- Are we using electronic signature capabilities where appropriate?
- Are we using proof-of-delivery capabilities where appropriate?
- Are our anti-virus, anti-spam and anti-malware capabilities sufficient to protect our organization from dangerous or unwanted content?
- Have we implemented DLP capabilities that will monitor outbound content through any channel, including removable media, and prevent sensitive or confidential information from being leaked inadvertently?
- Are we encrypting content where it is necessary or advisable to do so?
- Are our policies sufficient to meet our requirements for content management, encryption, DLP, etc.?
- Do we have a strategy that will sufficiently address every platform used in our organization, including email, social media, instant messaging, Web browsing, desktop computers, laptops, tablets, employees' personally-owned devices, etc.?

Summary

This white paper has offered a rapid survey of many new communication, collaboration, and content technologies that promise significant benefits for small businesses. Small businesses face unique challenges in comparison to their enterprise counterparts, and improving IT performance in such cases often revolves around embracing cloud-based and other fit-for-purpose services.

- With respect to communication, email retains a key position in the performance of work. Small businesses can switch their email infrastructure to offerings from smaller vendors, and achieve significant cost savings and flexibility enhancements. Unified communication services also promise to simplify communication activities for employees, while in parallel reducing capital costs, operating expenses and infrastructure complexity on the backend.

- Real-time collaboration services offer many tangible benefits to small businesses, not the least being the opportunity to shrink real estate requirements as employees work from any location without losing the ability to know what's going on inside the firm. Decisions can be made more quickly, while ensuring input from all relevant participants. To gain these benefits and eliminate the risk of using public Internet services, small businesses should deploy business-grade systems.

- Content management covers a plethora of technologies that offer more effective and efficient ways of running a business. From creating a backup infrastructure that works even when a primary business site is destroyed, delivering a synchronized file and document sharing service for collaboration, and gaining legally admissible proof-of-delivery for essential messages and documents, there are many great options for re-thinking the delivery of IT in the face of increasing competitive challenges and shrinking IT budgets.

- Staying safe and protected through well-considered security policies is the responsibility of every business, large or small. Anti-virus, anti-spam and anti-malware protection should be used by every business, without fail. The risks are too great to take a blasé approach. Additional security capabilities, such as data leak protection and content encryption should also be considered, with solutions deployed where risk must be mitigated.

- While many organizations focus on protecting their email systems against threats, they must pay equal attention to the security of their instant messaging, microblogging and social media systems given the growing threat that unmanaged use of these tools represents.

- The introduction of cloud-based services for communication, collaboration, content management and security offers tremendous benefits for small businesses. Services that were previously too expensive to deploy via on-premises infrastructure can now be gained in a cost-effective way, whether for short- or long-term requirements. Every small business needs to stay abreast of cloud developments because these offer a range of tangible benefits that were previously inaccessible.

In closing, there are many vendors that can help small businesses respond effectively to the competitive challenges at play in the market today, and use IT for competitive advantage and differentiation.

Sponsors of This White Paper

Cleartext delivers reliable, secure, standards compliant communication, collaboration and enterprise social networking solutions with customer service as our key motivator.

Cleartext
Level 26
44 Market Street
Sydney, NSW 2000
Australia
Tel: +61 2 9089 8957
www.cleartext.com

We draw on the knowledge of a team that covers the breadth and depth of the IT messaging, social business and security spaces across three continents.

We've been delivering business communication, collaboration and social solutions since 2005, bringing these technologies into a business with adequate policy, compliance and security tools.

Our enterprise social messaging platform, Cleartext EIM 2.0, delivers real time one to one chat, group chat and enterprise microblogging that helps increase productivity by fostering the creation of communities in the workplace.

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC) is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.

McAfee, Inc.
2821 Mission College Blvd.
Santa Clara, CA 95054
Tel: +1 888 847 8766
www.mcafee.com

Safend, a leading provider of endpoint data protection, guards against corporate data loss and theft through its content discovery and inspection, encryption and comprehensive device and port control. Safend encrypts internal hard drives, removable storage and CD/DVDs and provides granular port and device control over all physical and wireless ports.

Safend maps sensitive information and controls data flow through email, Web, external devices and additional channels. Safend ensures compliance with HIPAA, PCI, SOX, BASEL II and other regulatory data security and privacy standards. Safend solutions are deployed by multinational enterprises, government agencies and small to mid-size companies across the globe. For more information, visit www.safend.com.

Safend, Inc.
2 Penn Center, Suite 301
Philadelphia, PA 19102
Tel: +1 215 496 9646
Fax: +1 215 496 0251

Safend Ltd.
32 Habarzel Street
Tel Aviv 69710
Israel
Tel: +972 3 644 2662
Fax: +972 3 648 6146
www.safend.com