An Information Technology Update for Small Businesses in Eastern Europe

Small businesses striving to incorporate information technology [IT] into their operations are faced with a daunting array of choices. Complicating their decisions in recent years is a surge in broadband deployment, accompanied by a heightened awareness of security issues. In this whitepaper IntelliClear examines a number of recent technology advances and their impact on small businesses, together with an update on the utility of PCs and their performance in a security-conscious world. IntelliClear was commissioned by Intel Corporation to develop and publish this whitepaper, which represents the views and opinions of IntelliClear without influence or bias to the views and opinions of any vendor or client.

The Purpose of this Whitepaper – Examining Selected Small Business Technology Trends

Eastern European-based small businesses (less than 100 people) are becoming robust investors in technology, driving efficiencies and advantages that help them thrive in an increasingly competitive world. Unlike large corporations, small businesses don't often have on-staff experts to study new developments and determine which technologies will provide the highest return on their investments. The purpose of this paper is to provide small business decision makers with valuable insights into the latest technologies found in today's business PCs and the impact of those technologies on the security, data reliability, and efficiency of the small business.

Why Small Businesses are Purchasing Technology at an Ever-Increasing Rate

Using PCs can help small businesses reduce overall operating costs, be more competitive, and grow. AMI-Partners, a New York based research firm specializing in the global Small and Medium Business (SMB) market, reported in June, 2005 that "through adoption of IT and communications technologies and solutions, SMBs have emerged from a competitive disadvantaged stage during much of the 1990s to a level playing field today" versus large corporations. AMI states that as small businesses move to higher levels of IT adoption, "they seem well poised to evolve to a competitive stage with larger enterprises, due to a combination of IT and Web-enabled solutions, characteristic agility, and organizational efficiencies."[1] Consequently, as the adoption of PCs increases, those small businesses who are delaying the adoption of PCs are facing increasing competitive challenges, business difficulties, and vulnerability to failure.

AMI estimates "that much of the (small business) growth will occur in the Asia-Pacific region and Eastern Europe, where developing economies such as India, China and Russia are continuing to spur the creation of new businesses — many of which are buying PCs and servers as they build out their IT infrastructure."[2]

According to John Madden, Practice Director at Summit Strategies, a Boston-based consulting organization, "Technology investments by SMBs to increase productivity will continue. Small and medium businesses want the technology capabilities of large enterprises to improve their operations, but also because many of their customers and suppliers are demanding it."[3]

"Competitiveness is a key advantage of PC usage for small businesses, but also cost savings and growth are important benefits of PCs too," says Erhan Adali, Small Business Coordinator of Garanti Bank in Turkey. "For example, a small business direct marketer and advertiser was recently discussing with me that if they didn't use PCs with Internet access, they would have needed to hire more employees," says Adali.

A small business with PCs, broadband access to the Internet, email, and business applications that help facilitate such activities as accounting and marketing, can be exceptionally efficient no matter what industry they operate in. Small businesses that embrace the latest in information technology will clearly out-maneuver those

that don't, having a distinct advantage in capturing on-going commerce opportunities.

"Small businesses have more problems when they don't use PCs… lack of PCs makes employees work harder and consequently slows business growth and their ability to compete," says Sergey Chulin, Deputy Director of Binec, a government organization that provides IT consulting to small businesses in Russia. Mr. Chulin's comments remind us that for a small business, the centerpiece of a viable competitive and operational strategy is the PC. From the development of flyers and other demand-generating marketing materials, to the use of accounting software and spreadsheets for financial analysis and on-going process improvement, well-performing PCs enable small businesses to manage their operations more effectively.

Security Threats and Viruses Should be Taken Seriously, but Should Not Delay the Adoption of PCs

According to the Connecticut-based Gartner Group, "50 percent of all small and midsize businesses will go out of business within three years if they can't get back their data in 24 hours (following a major loss of critical data)."[4] For small businesses using PCs, security threats such as viruses and hacker attacks can seriously disrupt computer-based business operations. For that reason, it's important for small businesses to be proactive about keeping security and application software up-to-date to minimize potential disruption of their business.

"Of course being proactive is crucial, because the loss of data from a PC is a serious problem. Most small businesses are aware of this, with many having to experience a stoppage of their work process for half a day or more before investing in anti-virus software," says Przemyslaw Kadizioch, Executive Manager and Board Member at Optimus S.A., an IT consulting firm and reseller in Poland.

Up-to-date security software is a key element of an optimized security infrastructure. Regular updates can be facilitated through software subscriptions with manual and/or automatic updating capabilities. A more effective method available to small businesses is the use of Intel*

Active Management Technology (Intel® AMT), now built-into some PCs that utilize Intel® processors. Intel AMT allows technology support providers to proactively check and update software remotely from a central location.

Despite the anxiety to small businesses, viruses and other security threats can be easily avoided and are not sufficient reasons to delay the adoption of PCs. "PCs are far too important to small businesses to be stopped by viruses and other security threats. These threats should not deter a small business from purchasing PCs for their business,"" says Alexander Beresnikov, Executive Director of Ekoart, a computer reseller in Russia.

Symantec Corporation recently counseled small businesses: "Even the smallest of businesses are not immune to Internet threats… The introduction of new technologies, along with the increasing sophistication of Internet threats, calls for a defensive in-depth solution."[5] A comprehensive security strategy is achievable by small businesses and includes hardware, software, and policies that address common points of vulnerability.

Buffer Overflow Viruses and Worm Attacks are Common but Can be Prevented

According to a March, 2005 Internet Security Threat Report by Symantec Corporation, buffer overflow attacks, such as the now infamous "Slammer" and "Blaster" outbreaks, were the third most common attack in the 2nd half of 2004 and appear to be on the rise today.[6]

Effective protection against these attacks can be found today within the PC itself. Execute Disable Bit, a built-in feature of Intel processors, works with Windows* XP Service Pack 2 to guard against the entire class of viruses and worms that infect computers using this "buffer overflow" technique. The Bit prevents this malicious software from executing and possibly propagating to the network and other computers.

"Buffer overflow viruses are quite widespread," says Viktor Valchuk, an IT consultant with the Russian Chamber of Commerce Association of Traders and Producers. "Protection from such viruses can happen very effectively

IntelliClear
Bringing Clarity to IT Market Intelligence

with anti-virus programs," says Valchuk. Preventing buffer overflow viruses and worms is indeed a valuable form of protection for business PCs.

Other Tips and Technologies for Maintaining a Secure Environment

While security and anti-virus software is crucial in protecting a small business from disruption, it is ineffective if it interferes with the user's ability to get their job done, or fails to operate due to user intervention.

"Virus scanners do slow down the operation - I have seen it in many small businesses including my own. It especially affects employees who communicate or interact with customers. Clearly having faster, more streamlined security software and hardware would be great in order to solve this problem," says Lutfi Aygulen, Chairman and Owner of Balnak, a well known transportation company and member of the International Transportation Association in Turkey.

While PC performance is critical in keeping small business employees productive, it is also critical in keeping small business employees from tampering with security software. Alexander Beresnikov adds, "This kind of tampering does occur often, not only at small businesses, but at larger enterprises as well. It is important to have some way to avoid this tampering."

Microsoft, in a May 2005 support article, comments that turning off virus protection and/or firewalls can leave systems vulnerable to and unprotected against virus attacks and infections.[7]

The issue of performance and security software tampering can be managed by ensuring users are provided with PCs that can adequately perform under the strain of virus scanning and other security related computing overhead. Small businesses shouldn't underestimate the overhead that state-of-the-art security software can put on a PC. Squeezing an additional one to two years out of a two to three year PC life-cycle may not be a wise choice and could result in lost productivity. Small businesses should insist on PCs that are designed for business and are equipped with processors that provide plenty of head room for growth and security software overhead.

With so much attention on PC security, it's easy to forget about the issue of basic user access rights and authentication. The ability to control business access to files and networks, to those with need-to-know rights and the skills to handle the data, is critical so as to ensure privacy of employee and customer data, avoid sabotage, and reduce the potential issues in case of physical theft of computers. Symantec urges businesses to restrict and control network access by maintaining and enforcing firm policies.[8]

According to an AMI SMB study in 2004 a large percentage of SMBs were expected to hire new employees within a 12-month period.[9] With the upswing in new recruits comes the vulnerability associated with more users, more access, and an increase in the potential for malicious activities.

"Securing information against theft is critical to small businesses. I know a small business in Russia where an employee who had helped develop a database with client information and other data, left the company and stole that database so as to start his own company," says Viktor Valchuk.

The Role of External Service Providers

Capitalizing on the widespread attention focused on security, a variety of vendors and service providers are offering products and services to help prevent infections and security breaches, giving small businesses a multitude of choices in protecting their business. "Service providers would be useful to small businesses in such a role, because they would provide small businesses with security and a simple, easy-to-use service. For many small firms it is hard to ensure that a competent person is taking care of its security. Service providers could perform these functions and could do it cheaper than the cost of employing a specialist by the company," says Dariusz Podyma, Vice President of Wroclawska Agencja Rozwoju Regionalnego in Poland, a regional development agency in

Wroclaw where Mr. Podyma frequently interacts with small business CEOs.

Service providers play a critical role in ensuring small businesses are adequately protected, and receive help to quickly recover in the event a breach does take place. Market research firm, AC Nielsen, reports that "a growing number of SMBs in the United States are turning to a trusted service provider to design, install, and maintain their security solutions."[10] In a 2004 study in North America research firm Infonetics reported that "more than 38 percent of small businesses and 50 percent of medium-sized businesses get one or more of these essential security functions - virus scanning, firewall, authentication, VPN client, and intrusion detection and prevention - from a service provider."[11] IntelliClear believes that these same service provider trends will evolve in Eastern Europe at an increasingly accelerated pace.

With the help of a service provider, small businesses can develop a comprehensive security strategy utilizing existing capabilities of the operating system, and hardware components found in business-class PCs. Experienced service providers can also evaluate information access policies and procedures to uncover physical vulnerabilities, and recommend additional security software if necessary.

Businesses should look for service providers that have remote support capabilities that allow them to examine, troubleshoot, and repair systems over the network. Remote support capabilities provide small businesses with not only timely resolution of problems, but potential cost savings due to fewer on-site technical service visits. Large corporations have been using remote management capabilities for years to support their IT infrastructures, reduce costs, and preserve precious IT resources.

These remote services are extending to the management of software environments. Features that enable service providers to assess and update software on networked PCs can help keep security software up to date; allow for the understanding of what software is installed to advise on its ability to handle business growth; identify how many copies of software are in use in order to minimize licensing costs; and identify which versions of software are installed in order to assess the PC's capability to meet regulations for privacy and accurate financial reporting.

In the past, remote services were limited by an inability to operate on PCs that were powered off or were unable to boot. Intel AMT provides the ability to diagnose problems, replace system files, update security software, and restore systems to normal operation even when the PC is turned off or the operating system cannot be started. This capability is available only in systems using Intel chips.

These remote service provider operations are likely to become more common as broadband becomes ubiquitous and Internet-based services reach the mainstream. As this happens, remote management of PCs will be a valuable service for small businesses. With respect to remote PC management Tunc Avkut, Co-Founder of Tubider, an IT Association in Turkey providing consultation, guidance, and direction on a variety of IT related matters for small businesses, comments: "About 100 service providers in Turkey currently offer remote PC support. It saves time for small businesses, while service providers can provide a better service from a timing and technical perspective - especially concerning virus problems."

A Second Hard Disk — Simple Insurance for Data Protection

For data protection, having a second hard drive in a PC continuously copying information from the primary hard drive can be invaluable. This feature can provide data redundancy in the event of a system or hard drive failure. Until recently, this capability, known as "disk mirroring," required a special add-in card and software. But this year Intel has begun building this feature, called Intel® Matrix Storage Technology, into chips used in business-class PCs.

"Use of a 2nd hard disk drive is a common practice among small businesses in Russia. It is not a critical factor cost wise since hard disk drives are inexpensive relative to the cost of the PC." says Alexander Beresnikov of Russia.

IntelliClear
Bringing Clarity to IT Market Intelligence

Voice Over IP (VoIP) Enabled Through a PC, Delivering a Better Telephone

Voice over IP (VoIP) technology sends telephone calls over the internet, often at substantially lower costs than regular telephone calls. Worldwide SMB IP Telephony (VoIP) spending is expected to grow at a CAGR of 41 percent from 2003 to 2008, reaching an estimated total spending in 2008 of $4.5 billion according to AMI.[12] Many small businesses have already surmised that cost savings and efficiency gains are just the start of how VoIP can benefit their business.

One particular implementation of VoIP is the use of "PC soft-phones," software that acts like a telephone and runs on a PC. PC soft-phones using VoIP (e.g. services such as Skype*) can help businesses serve their customers better and operate more efficiently by streamlining communication, reducing costs, while enjoying high-fidelity voice quality on PC-to-PC phone calls.

"VoIP can reduce costs and help small businesses operate more effectively. It seems that this will soon replace traditional technologies such as the telephone. Cost reduction is the main advantage of using PCs as telephones. I think this change is inevitable, as for a small business it is a matter of tens or hundreds of thousands zlotys per year," says Przemyslaw Kadzioch of Poland.

Conclusions – Educate, Plan, and Invest

The opportunities for small businesses to improve their operations through the effective use of information technology - mainly the new breed of business PCs equipped with advanced Intel processors - are enormous and multi-dimensional. A number of valuable new technologies relating to security, remote support, reliable data redundancy, and VoIP have been recently introduced and will help small businesses capture these opportunities through disciplined education, planning, and investment. By working with solution providers small businesses can deploy these technologies and gain the benefits associated with ongoing effective technology usage.

IntelliClear recommendations:

1. Keep security software up-to-date.

2. Maintain optimal security including anti-virus software, Microsoft* Windows* XP Service Pack 2, and Intel's built-in Execute Disable bit technology.

3. Choose PCs that are designed for business, with performance enough to prevent security software from interfering with user computing tasks.

4. Select a service provider who can help with security and remote computer support.

5. Insist on PCs with Intel® Active Management Technology for better remote support.

6. Protect business information with Intel® Matrix Storage Technology and a second hard drive.

7. Deploy PC-based VoIP to reduce costs and increase business efficiencies.

About IntelliClear (www.intelliclear.com)

IntelliClear is a market research and business consulting firm committed to the delivery of actionable market intelligence to the global IT community. IntelliClear's mission is to bring clarity to IT market intelligence by delivering results-oriented research, responsive industry experience, and effective data synthesis - leading to confident go-to-market plans. IntelliClear leverages the experiences of seasoned IT and market research professionals, while utilizing its global network of industry consultants and research partners to execute projects across a broad spectrum of disciplines and geographies.

References:

[1] Bose, Anindya, Sahni, Deepinder (2005). *The Large Potential of the Small*. *SAP INFO, No. 129*. Retrieved October 10, 2005, from Hhttp://www.sap.info/public/INT/int/index/PrintEdition-1147542c01a622792b-int/-1/articleContainer-1444142c3db1144dc0H

[2] AMI-Partners, Jul 2004 – SMB IT and E-Business Spending Report. Retrieved from eMarketer on October 10, 2005 at Hhttp://www.emarketer.com/Article.aspx?1003223H

[3] (2004). *Saving Grace*, Retrieved October 8, 2005, from CMP Media Small Business Advantage Knowledge Center website: Hhttp://www.thesmbadvantage.com/document.asp?doc_id=1011H

[4] Gartner quote as found in an NSi Software Whitepaper *Six Tips Small and Midsize Businesses Can Use to Protect Their Critical Data*, 2003; Retrieved October 10, 2005 from Hhttp://www.zdnet.co.uk/i/z/wp/SMB_6_Tips_23.pdfH

IntelliClear
Bringing Clarity to IT Market Intelligence

[5] *Defense in Depth and Your Small Business*, Symantec website article (2004) Retrieved October 10, 2005 from Hhttp://www.symantec.com/smallbiz/library/depth.htmlH

[6] Symantec *Internet Security Threat Report Vol VII*, Mar 2005. Retrieved October 10, 2005 from Hhttp://ses.symantec.com/pdf/threatreportVII.pdfH

[7] Microsoft, May 2005 – *How to Turn On or Off the Firewall in Windows XP.* Retrieved October 10, 2005 from Hhttp://support.microsoft.com/kb/283673H

[8] "Defense in Depth and Your Small Business", Symantec website article (2004) Retrieved October 10, 2005 from Hhttp://www.symantec.com/smallbiz/library/depth.htmlH

[9] Bose, Anindya, Sahni, Deepinder (2005). *The Large Potential of the Small. SAP INFO, No. 129.* Retrieved October 10, 2005, from Hhttp://www.sap.info/public/INT/int/index/PrintEdition-1147542c01a622792b-int/-1/articleContainer-1444142c3db1144dc0H

[10] AC Nielsen study of US SMBs, 2004 as printed in Cisco White Paper *Managed Security for the Small and Medium Business*, retrieved October 10, 2005 from Hhttp://www.cisco.com/en/US/netsol/ns458/networking_solutions_white_paper0900aecd8028bc06.shtmlH

[11] Infonetics *North America User Plans for Security*, Nov 2004 as printed in Cisco White Paper *Managed Security for the Small and Medium Business*, retrieved October 10, 2005 from Hhttp://www.cisco.com/en/US/netsol/ns458/networking_solutions_white_paper0900aecd8028bc06.shtmlH

[12] Data is from the September 2004 AMI-Partners' report titled The SMB Global Model. Retrieved from the eMarketer database on October 10, 2005