Infosecurity europe

A selection of papers from exhibitors at Infosecurity Europe 2007, Europe's dedicated Information security event. Now in its 12th year, providing an education programme, new products & services, over 300 exhibitors and 11, 600 visitors from every segment of the industry. 24th-26th April 2007, Grand Hall, Olympia. www. infosec. co. uk

Small and medium-sized businesses represent the most dynamic and most rapidly growing segment in the country, and the very survival of our economy is dependent to a large degree on the success of these businesses. SMBs, whether they have five employees or a hundred, are more tech-savvy than ever, and their increasing level of technology spending is destined to make the SMB segment much more competitive. SMBs are more willing to make the capital expenditures it takes to create the technology infrastructure they need to compete on a global level. The National Federation of Small Business indicates that two-thirds of small businesses surveyed made capital expenditures over the past six months.

But of all those capital expenditures, technological infrastructures and equipment spends, the one that technology managers dislike most and often neglect is backup, archiving, storage and disaster recovery planning. The benefits they bring are not readily obvious, and in the best-case scenario, backup and recovery is something you never have to use. Yet, whether you save your files to floppy disks, to tape, CD, or to a redundant drive, backup remains essential.

Small to medium sized businesses (SMBs) in particular are starting to pay attention, as these smaller organizations attempt to position themselves on

a level playing field with larger companies as they compete in the global marketplace. A host of new regulations have started to govern our IT infrastructures, and SMBs face an unproportionately larger burden of compliance. Many of these regulations govern how data is stored, archived and accessed. Although SMBs are using data storage, archival and recovery systems more frequently, they are often less than adequate. Archiving data files to tape or a CD may be well and good, but it's only a partial solution.

A SPIT in the ocean

Executing tape backup on a regular basis is a manual-intensive process that is a poor use of skilled manpower. Does it make sense to have a $50, 000 a year IT staffer pushing around racks of tape into storage all day? The costs in labor alone are enormous. Tapes have to be rotated manually and physically transported to an offsite location for storage. Retrieval is an even bigger headache. Statistics reveal that over 30 percent of IT costs are associated with backup. And besides the time and expense factor, because it is a manual process, it is prone to error, and data recovery from backup tapes fail an alarmingly high number of times. In addition, recovery is notoriously slow, up to 400 times slower than recovery from disk.

The most common practice is to archive data partitions on a daily basis. This creates a Single Point In Time (SPIT) image of the network data, which is of limited use. From this SPIT backup, it is possible to recover a file that existed prior to the previous day's backup, but what happens when you spend all day on a file, your system crashes, and you lose your data the same day? It's gone forever. There is no backup. This snapshot approach to backup can be

useful, but it is limiting. There may be thousands of transactions that take place during the day, and relying on a once-daily tape backup can still result in a massive loss of information and revenues. While most agree that tape backup has its limitations and flaws, still 75 percent of SMBs still use the fixed schedule tape systems despite the fact that they are difficult and time-consuming to manage, prone to error, and unreliable. Fortunately, industry trends show that costs of more sophisticated archiving and disaster recovery systems that afford continuous data protection and the possibility of a full, bare metal recovery are fast becoming affordable, even for smaller businesses.

Business continuity and the SMB challenge

Any data-intensive company requires some level of business continuity, and this calls for a more sophisticated approach to backup, recovery and disaster planning. SMBs are now placing their IT storage infrastructures on the top of their priority lists, and spending more on these processes.

SMBs face an increasingly high number of factors, including more data requirements than before, due to an increased dependence on e-business and networking. Adding to the pressing need to protect business data are a rapidly growing collection of regulations, including HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley and other regulations from the SEC, NASD, and individual states. SMBs must necessarily move towards more high-end archival and backup solutions than they would have considered previously. Fortunately, the industry has stepped up to the plate with an array of solutions targeted specifically at this market.

However, backup without the ability to recover is of little use. SMBs can now go beyond the limitations of tape archiving to achieve " *Any Point in Time* " recovery. The combination of continuous data protection, offsite data backup, and bare metal recovery affords the greatest protection and forms the foundation of a workable disaster plan. These factors combined can make the difference between getting back in business after a disaster--or suffering losses to monumental that economic recovery is impossible.

Pedal to the metal: Going beyond the daily backup

In the aftermath of the devastating Hurricane Katrina businesses that had planned ahead with disaster recovery strategies were able to get up and running within days, or even hours, keeping their losses to a minimum. Others suffered huge losses, and the losses were so extreme that hundreds of small and medium-sized businesses had to close their doors permanently.

So you think your small business is doing well because you back up your data once a day? In fact, you're just a day away from disaster if that's the case. In disasters like Katrina, business recovery required much more than restoring data. Entire systems may have been destroyed. Just having a data backup may well be useless, if the computers and applications have also been compromised. Disaster recovery, sometimes referred to as " bare metal" recovery, restores the entire system, including operating system, user and system settings, applications and data. The ability to execute a bare metal recovery is lacking in many backup and archiving systems, particularly those targeted towards the SMB sector. Most SMBs, faced with a system-wide disaster, must execute the bare metal recovery manually, a

process that takes days. It involves re-installing the OS and all applications, re-configuring all user and application settings, and literally transforming each PC, workstation and server from " bare metal" to a functioning computer again. SMBs can ill afford the loss of computing for days on end while the process is executed manually. The loss of business and revenue could be enough to put a small business out of business. It's time to plan ahead, and time to go beyond the basics.

A Disaster Planning Strategy

Today, it is possible for SMBs to have an enterprise-style disaster recovery system on an SMB budget. A good disaster recovery plan has several elements, not the least of which include having an alternate physical location for office space. But the most important element of disaster planning involves recovery of computer systems. This is not limited to a simple " snapshot" data backup. The entire system, including operating system, user and system settings, configuration information, applications, and data must all be redundant and backup must be continuous. Today's SMB recovery systems must involve a system of instant and continuous backup, which commits data and transactions simultaneously to a local archive and a secondary archive, preferably off-site. There are three components of a good SMB disaster recovery plan:

- Continuous data protection
- Offsite data backup and storage
- Bare metal recovery capability

Data protection must go beyond snapshots to avoid losses and preserve more recent data. In addition, both local and offsite data protection is recommended. While a local archive provides for fast restore of individual files, the offsite data protection affords protection against major disasters that could affect the physical location of your computers. Offsite archiving is often required to restore snapshots of data for long period of time, to meet compliance regulations.

The rapid digitization of content, the blurting of corporate boundaries, and compliance regulations have created an environment where today's SMB must acquire, maintain, and protect massive amounts of data. Older SMB solutions simply aren't up to the task. Fortunately, disk costs have decreased to the point where inefficient " snapshot" style tape archiving is no longer necessary, and even the smallest business can afford to establish a system of continuous backup--and be prepared for any disaster.

Keeping a tight lid on Pandora

Freddy Mangum, VP of Product Marketing at Fortinet

The quest for greater ARPU has driven telecom services innovation and brought about new open-standards based network architectures for fixed and mobile/wireless operators. This evolution towards IMS has opened a Pandora's box of security risks as telecom carriers come face-to-face with threats they were previously shielded from when they deployed closed and proprietary circuit-based networks.

Carrier security is an issue rarely discussed in public, although the security stance among mobile network operators is actually very encouraging. As an

industry, mobile operators treat the issue proactively, taking steps to protect entire core services infrastructures rather than merely leaving subscribers responsible for protecting their smart phones.

While altruism may well be a factor, the main reason for this posture remains ARPU. Mobile operators are on the cusp of realising truly mass-market penetration for pre-IMS (2. 5G) services such as MMS that deliver advanced ringtones, games etc., and widescale disruption could mean those revenues (as well as accumulated brand equity) falling off a cliff. Market competition demands differentiation, and no mobile operator wants to be the odd-one-out when it comes to security--particularly with 3G, 4G, FMC and all-IMS networks looming so large on the horizon.

It's easy to underestimate the threat posed by mobile 'malware'. Criminal entities hardened by experiences in the fixed Internet world have emerged and seek to defraud subscribers and/or carriers in an effort to extort monetary gain. Their activities have grown exponentially since 2004/2005 so that today, anything up to 5% of all mobile network traffic is currently being infected with some form of malicious code. Hackers typically gain access to pre-IMS networks through the application layer and silently exploit individual subscribers in the following ways:

Malicious Attack. Exemplified by the Skulls virus, this group of malware seeks to completely disable the infected device by removing or corrupting its system functions.

MMS Spam Threat. This involves cyber criminals posing as legitimate promoters of an illegitimate service or prize draw. Having mass-mailed MMS

message describing the promotion, individual recipients are invited to download an application installer in order to participate. Once installed, this software replicates itself to every number in the device's phonebook before sending unlimited numbers of texts to the advertiser's account, thereby generating huge amounts of revenue. Victims only find out when they receive their monthly bill, or run out of credit.

MMS Service Threat. Similar to the threat above, this involves the richer media file structure inherent within MMS, capable of attaching application files (such as games), which can harbour malicious code. Examples include ComWarrior and Mosquito. MMS messages are also most likely to carry offensive, unsolicited content designed to cause maximum distress, particularly among juvenile users.

Smart Phone Web Browser Application Threat. This approach represents apparently normal applications that obscure a sinister side. Examples include RedBrowser, a free-of-charge messaging application containing a Trojan program that directs each message to a $5-a-time premium rate number.

The opening up of the network and the growth of standard-based devices--both developments designed to facilitate greater services innovation and flexibility--have created challenges for mobile operators both at the application service layer and deeper at the core-IP network layer. Laptops, PDAs and smart phones that traverse fixed and mobile networks can cross-pollinate any threat developed through the medium of IP.

Defending pre-IMS networks therefore involves more than merely putting up network roadblocks. Operators understandably worry about network

performance, service uptime and its effect on user experience, therefore care must be taken to ensure that legitimate network traffic is not delayed or mistakenly terminated. An effective security solution must analyse all traffic, make an appropriate determination in separating the good packets from the bad, and take action in 'real-time' to thwart nascent security risks well before they can impact network performance or disrupt service delivery.

Hackers are applying knowledge gained from years of attacking users on the fixed network to conceive highly sophisticated mobile threats that can easily confuse or overwhelm security systems focussed on countering specific types of threats. If these were just viruses, then the obvious solution would be an anti-virus filter. Unfortunately these blended threats often combine the characteristics of a virus, a worm, a DoS (Denial of Service) attack, blacklisted content or spyware, and they can morph very quickly once launched by the hacker.

Any deterrence solution therefore should employ a combination of identification and multi-layered analysis techniques coupled with rich, up-to-date security content to minimise false positives (where normal traffic wrongly triggers a response) and false negatives (where actual threats are missed) across the network. This approach centres upon taking full advantage of new technology advances to flexibly implement real-time application and core-IP layer protection from the full gamut of security functions; MMS antivirus, anti-spam, GTP firewall, web and content filtering, IPS, VPN etc. A flexible and modular yet unified approach in this regard is also critical, particularly in light of mobile operators' understandable sensitivity to the prospect of escalating operating costs or management

overheads. Operators understand that securing their current pre-IMS infrastructures is the surest path to ensuring safe migration to tomorrow's advanced, converged SIP-based applications and services. It starts with the implementation of a proven, high-performance carrier-grade (e. g. AdvancedTCA certified) platform, configured to be constantly abreast of new multi-threat intelligence and capable of ensuring effective management and analysis. It carries on down the road to greater ARPU and lower risk.