NOW YOU SEE IT,THERE IT... STAYS

Decreasing business costs and risks of costly data loss

We live in a 24/7 global economy that is more dependent than ever on technology. Even the technology of small and medium sized businesses (SMBs) houses sensitive digital data - employee and customer information, internal emails, documents and financial records, sales orders and transaction histories. Not to mention applications and programs critical to daily business function and services.

Employees at SMBs require continuous access to the critical business data needed to meet the demands of the customers or clients they service. They even want this access while they're at home or on the go running errands.

To satisfy this demand, many companies and organizations now allow employees to BYOD (Bring-Your-Own-Device) and "do business" using their personal laptops, tablets and mobile phones. The web, Wi-Fi networks and mobile devices with robust memory and battery life have made this constant access to a SMBs back office infrastructure a reality. Regrettably this flexibility and freedom is accompanied by an ominous risk of data loss.

Just a single data loss or breach can be costly to SMBs. Data losses and leaks come with lingering continuous costs that many SMBs cannot easily shake or overcome. Revenue is lost if employee productivity and customer accessibility/ service are stalled by data loss. The expenses associated with internal research and investigation, system repair and maintenance, and data security protection are another heavy price SMBs must pay. If cybercrime is involved, affected customers must be notified, the potential exists for litigation, and many customers will likely never return due to mistrust.

While corporate-level data losses are well publicized, many SMBs mistakenly believe their data isn't at risk. This mistake can prove to be a costly one.

NOW YOU SEE IT,THERE IT... STAYS

Why C-Suite Management at SMBs Can No Longer Ignore Data Loss

- Following a significant data loss, it is estimated that SMBs can lose up to 25% in daily revenue by the end of the first week.

- According to the *National Archives & Records Administration in Washington,* 93% of companies that have experienced data loss, and prolonged downtime for ten or more days have filed for bankruptcy within twelve months of the incident. 50% wasted no time and filed for bankruptcy immediately. 43% of companies with no data recovery and business continuity plan actually go out of business following a major data loss.

How quickly can your business be restored if critical data is lost? When was the last time backup processes were tested to ensure all data is recoverable and business operations are quickly restored?

- A survey conducted by *Symantec* SMB revealed that fewer than half of SMBs surveyed backup their data each week. Only 23% of those surveyed said they backup data every day and have a business continuity plan in place.

- The percentage of cybercriminal attacks targeting businesses with fewer than 250 employees doubled in 2012. The vulnerabilities of naive small business owners have been noted, and hackers have now placed the proverbial bull's-eye on these perceived weak links. If sensitive customer data is leaked, SMBs may face overwhelming financial liabilities, which could include reimbursing affected customers and legal fees.

- BYOD isn't a trend or passing fad. It is here to stay and the fact of the matter is businesses no longer own the devices used by employees. This is unprecedented. It's not as if the employees of yesterday could haul home their file cabinets and desk. This obviously comes with a number of data security risks. The number of networks, applications, and end points where data can be accessed has multiplied with BYOD. Who manages these devices? Who secures these devices? Do SMBs have the right to back up data on machines they do not own? If an employee loses a laptop,

or goes AWOL on the company, what data do they have and does anyone else in the company have access to it?

Management Is On Notice

Businesses today are playing on a much bigger playing field than they were two decades ago. Any SMB that trusts the security and backup of critical business data with a limited and overburdened in-house IT team, or forsakes internal IT support altogether for emergency on-call help when things go bad (Break/Fix Mentality), is playing with fire and begging to be burned.

Any disruptive or invasive technological event - even the smallest of incidents - can have an amplified impact on day-to-day business and profitability. Being proactive with data recovery solutions, and having emergency response procedures in place prior to a disruption or data disaster, is the only way to get critical data restored immediately to the data center, minimize downtime, protect customer and client data and soften the impact of such events.

NOW YOU SEE IT,THERE IT... STAYS

Data Security Threats Every SMB Must Be Aware Of

Human Error and Employee Negligence

Human error, by way of unintentional data deletion, modification, and overwrites, has become much more prevalent in recent years. Much of this is the result of carelessly managed virtualization technology. Virtualization and cloud computing have enabled improved business continuity by allowing entire servers – including all data, operating systems, applications, and patches to be grouped into one software bundle or virtual server and subsequently backed up. The catch is humans must still instruct this technology how to perform, which is why so much of today's data loss is linked to human error.

The complexity of these systems often presents a learning curve that involves quite a bit of trial by error. For example, a support engineer can accidentally overwrite his backup when he forgets to power off his replication software prior to formatting volumes on the primary site.

While most CIOs at SMBs are generally accepting and understanding that mistakes happen, they must be more stringent when it comes to managing risky negligent employee behaviors in this era of mobility and accessibility. Employee negligence puts a company or organization's critical business data at risk of being stolen by cybercriminals or malicious employees. Examples of this negligent behavior include:

- Leaving computer systems unattended
- Weak passwords ("password" or "12345") or passwords that aren't frequently changed
- Opening email attachments or clicking hyperlinks embedded with spam
- Visiting restricted websites

NOW YOU SEE IT,THERE IT... STAYS

Employee Mobility & Data Exposure

In the modern-day BYOD workplace, more people are doing daily business on their personal laptops, iPads and Blackberrys. They are also carrying around portable media like thumb drives, USB sticks and CDs.

These devices are not always backed up or secured by IT administrators. There is not only the potential for these devices to be lost or stolen but there is also a very high probability that employees using them are also accessing personal email, downloading music, browsing the web, playing games and hanging out on Facebook. This makes sensitive data susceptible to malware, viruses and hackers. All of this substantially ups the likelihood of data loss incidents.

Four Ways SMBs Can Minimize Data Loss

- **Enforce Data Security** - This is more or less the managing of the "human factor." CIOs and those in SMB management roles must communicate data protection policies to staff and ensure their implementation. Rules must be set, particularly with personal devices, to enforce security policies. It can be as simple as sending reminders to not open email attachments from unknown sources, requiring passwords be reset every few months or the banning of specific file sharing or social networking sites.

In May of 2012, security concerns led to over 400,000 IBM employees being banned from using the cloud storage service Dropbox and Siri – the iPhone personal assistant. While far from an SMB, if IBM can go that far and make such a demand

to so many employees, a insurance agent can certainly remind his or her marketing representative to not play Farmville on Facebook if they're using a laptop containing company and customer/client data.

- **Stress the consequences** – both personal and business – of not properly protecting confidential data. Encourage employees to make passwords difficult to crack. Patch holes in the infrastructure's walls by identifying the most critical data. Perhaps a trusted IT advisor can help implement processes to better protect that data's security perimeters.

- **Mobile Device Management** – Mobile Device Management grants SMBs a semblance of control over the mobile devices used within the company. Devices tapping into company systems are identified and remotely monitored and managed 24/7. More importantly, they are proactively secured via specified password policies, encryption settings, and automated compliance actions. Lost or stolen devices can be located and either locked or stripped of all SMB-related data.

- **Snapshots** – Fully backing up large amounts of data can be a lengthy process. The data being backed up is also vulnerable to file corruption from read errors. This means sizeable chunks of data may not be stored in the backup and be unavailable in the event of a full restore. This can be avoided by backing up critical data as snapshots, which are read-only copies of data frozen to a specific point in time and stored using minimal disk space. These virtual snapshots are immediately available for restores in the event of data loss.

- **Cloud Replication and Disaster Recovery Services** – The cloud provides SMBs who consider data backup to be too costly, time consuming and complex with a cost-effective, automated off-site data replication process that provides continuous availability to business-critical data and applications. Cloud replication can often get systems back online in under an hour following a data loss.