

## Discussing Data Protection with Sumit K. Pal

**W**ith technology constantly evolving and advancing, security risks are on the rise. For many small and medium businesses today, protecting important data and maintaining a level of sound security to avoid breaches can be crucial to a company's success. But many businesses do not realize that their own organizational structure is often the root of allowing these risks to exist because companies lack a system of controls, responsibilities and planning to proactively address these issues.

For "non-accelerated" public and private companies (\$70 million in revenue or less) alike, allowing these issues to go unaddressed and unresolved can seriously compromise companies' ability to attain or maintain compliance with Sarbanes-Oxley (SOX).

*IT Defense Magazine* discussed these topics with Sumit K. Pal, the Executive Vice President of Operations for WithumSmith+Brown Global Assurance. Pal has more than 27 years of professional experience in business consulting and systems integration. He is responsible for IT Consulting, Human Capital Management and Project Team Management.

**ITD:** *What are the common business and IT challenges for SMB?*

**SP:** There is always an integrated and interdependent relationship between business and IT. Thus SMB's attempt to maximize their gains and values while optimizing their available pool of resources. For example, some of the typical struggles SMB's encounter include balancing revenue increases and profitability while reducing costs, manag-

ing exponential data growth while enabling effective and efficient access to it and delivering value to shareholders while increasing the value and quality of the business itself.

Overall, SMB's try to increase customer satisfaction and revenue creation with the continued pressures to optimize resources, meet tighter delivery schedules, and improve overall responsiveness.

**ITD:** *What are some of the most common IT issues that threaten non-compliance for small and medium businesses (SMB)?*

**SP:** SMB's usually find themselves at risk of non-compliance due to the lack of

proper scoping of applications relevant to Internal Controls (for the regulatory compliance involved) as well as the fact they have not properly segregated IT duties and have excluded any IT personnel from the project team at the onset of the process.

In addition, the absence of a comprehensive, high-level IT strategy to synchronize with the overall business strategy along with detailed IT plans and procedures and process documentation impedes compliance along with no adequate patch management procedures for the network and operating system(s) and upgrades for software applications in use.



**ITD:** *Why is it important for business owners to integrate technology into the overall corporate plan?*

**SP:** It is important as IT provides the platform to be able to build standardized, integrated, best-of-breed, sustainable business processes that all authorized employees can utilize – this leads to better risk management, increased productivity, improved revenues, reduced errors, controlled costs and so on. Secondly, this is the best way to ensure that the company derives the best ROI on their IT assets. Thus SMB must ensure that both business strategy and the IT strategy are in sync.

**ITD:** *What is the most common security vulnerability you encounter among small and mid-sized firms?*

**SP:** Network related vulnerability is probably the most common vulnerability encountered. Some of the key security challenges continue to be the increasing sophistication of attacks, employees not following security policy, the increasing complexity of security solutions and limited budgets that do not adequately cover the costs associated with effective security.

**ITD:** *From a SOX perspective, how should an SMB approach their compliance initiatives? Timelines? When should they get started?*

**SP:** SMB's need to realize that in reality, they should have already attained compliance due to the coming deadline of December 15th this year which states that SMB's need to be SOX Compliant (not just ready) and draft management's annual assessment of the effectiveness of Internal

Control over Financial Reporting (ICFR) for all companies reporting financials.

At the same time, the Independent Auditors' role would be to review the effectiveness of ICFR, not management's assessment of ICFR for financials reporting after December 15th of next year. All of this is of course subject to the current reviews being undertaken by the SEC and the PCAOB.

Small public companies have been warned not to use the time extensions to delay implementation, but to use it to improve the quality of their documentation. SMB's typically do not have adequate internal resources to be able to complete the tasks needed in-house so there is usually a greater reliance on external support to attain compliance.

**ITD:** *What are the benefits of SOX like IT controls for a SMB?*

**SP:** Some specific outcomes by embracing SOX include establishing documented policies and procedures including IT processes and controls, creating increased automated controls as against manual controls which generate significant cost savings for the organization and reducing the security risk and data privacy issues.



In addition, those SMB's that view SOX as not just a regulatory mandate but as an investment for future growth most likely know that compliance offers a better valuation for the firm (independent studies have indicated up to 13% more) and enable a greater ability to attract and complete mergers and acquisitions. SOX compliance is also a key component to generating interest from private and venture capital and affords firms to expand their business relationships and eligibility for contracts.

**ITD:** *What are the practical ways for SMB to protect their business?*

**SP:** Real business protection means far more than just keeping servers, PCs and networks up and running – and far more than the ability to recover from harmful events. It's also important that those systems be relatively easy to manage and capable of maintaining the integrity of your data.

**IT provides the platform to be able to build standardized, integrated, best-of-breed, sustainable business processes that all authorized employees can utilize — this leads to better risk management, increased productivity, improved revenues, reduced errors, controlled costs and so on.**

## Test and update your backup and recovery, security and availability systems every six months at minimum — even quarterly, if possible. Make sure these are real-world tests, not simulated exercises...

Some best practices, tips and ideas for real business protection that are applicable to SMB's include:

- Understanding your infrastructure. Track how many desktop and mobile PCs, servers, routers, printers and other physical equipment you own, what software you use (firewall, virtual private network, antivirus, etc.), and know how everything is used. Build a map showing where equipment is located.
- Creating a comprehensive backup and recovery strategy. Plan a series of meetings to review all aspects of backup and recovery, and think through as many threat scenarios as possible (natural disaster, power outage, theft, security breach, etc.). Take into consideration not only data on the network, but also PCs, mobile devices and applications no matter where they reside. Consider the time and resources required for recovery in all your scenarios and evaluate the business impact of downtime for various systems.
- Testing, backing up and restoring your system. Test and update your backup and recovery, security and availability systems every six months at minimum — even quarterly, if possible. Make sure these are real-world tests, not simulated exercises, and that all employees are both trained in disaster preparedness and capable of working at home or at an alternative site.
- Implementing a multilevel data protection model where appropriate. Multilevel protection recognizes the power of utilizing disk and tape together to provide a more effective and powerful data protection solution. Disk-based backup solutions can address many issues such as server backup windows and recovery speed, while tape is an essential foundational component for offsite and long-term archival. When considering offsite disaster recovery options, make sure there is plenty of distance between the location of servers and the backup location to reduce vulnerability to regional threats, such as flooding, earthquakes or hurricanes.
- Enabling remote server management and recovery. Cut operating costs, including travel time for support staff, by managing and supporting servers from a single location. This will also allow you to be proactive in assessing potential problems and respond in real time to actual problems. Make sure your server hardware and management solutions support this vital capability if you have servers in multiple locations.
- Mirroring your servers. Mirroring data and applications residing on two servers, on two additional servers or on one server plus attached storage (preferably in two different locations) is an important part of business protection. This approach provides you with an extra backup that's instantly available if something happens to one location. Look for mirroring solutions that automate both the mirroring and the use of one server if the other goes down. **ITC**