



Posted to the NaSPA.com website on Thursday, 06/14/2007

Security and Compliance Challenges for Small and Medium Businesses

By Sumit K. Pal

There isn't much time left for publicly listed small and medium businesses (SMBs) to be Sarbanes-Oxley (SOX) compliant as the deadline of December 15th approaches (unless of course this date is once again pushed back by the SEC as part of the current review process). This federal law, born in the wake of a series of scandals that shook the stock market and generated scrutiny over companies' accounting procedures and internal corporate governance, has already been in effect for "accelerated companies." This means publicly owned firms that have a net worth of more than 75 million dollars. Public companies under that mark fall into the "non-accelerated" category. But regardless of whether an SMB is public or private, businesses should take steps to ensure they have the right compliance infrastructure and policies in place to avoid risk.

Whether it is attaining compliance or simply day-to-day management, SMBs do have advantages over the 'big boys' including the fact they have fewer products to market, which increases their ability to focus on them. The smaller the business, the fewer levels of management they have to contend with, which includes fewer employees because many of them wear several hats, with a wide range of duties. There are several common mistakes SMBs make when it comes to complying with the Internal Control over Financial Reporting (ICFR), which is required for SOX. Reporting errors have been recorded in areas such as financial close processes, personnel and training, tax accounting, IT controls, revenue recognition, and mergers and acquisitions can occur. Given that such errors have occurred, there is one major disadvantage that many SMBs face that is probably the number one reason they are struggling to meet compliance or establish effective operations.

It all lies within the IT department. Most SMBs have a small IT department, in some cases a team of four members maximum. For others, IT may be completely non-existent on the premises and it may be outsourced from another company. This is where the security and compliance issues lie. In many cases, executive management underestimates the effort and resources that are necessary. Beyond the basic set-up, there is typically a lack of network security solutions and a lack of IT awareness. Also, there is a lack of documentation of IT policies, procedures, processes and controls as a result of the absence of an investment in this area.

What all this basically means is that SMBs are setting themselves up for non-compliance as well as operational ineffectiveness. They may not have a centralized experienced IT department to scope out the proper applications needed to regulate compliance and they also may not have people on board informed about procedures such as upgrading software and properly installing network and operating systems updates that they would need to be compliant.

Overall, business owners need to integrate technology into their corporate plan and build a standardized and sustainable business process that all authorized employees can use. This will lead to better risk management and the benefits that come from it including improving the bottom line. When it comes to security issues, lack of IT infrastructure can put businesses in very vulnerable positions. For example, the increasing sophistication of hackers alone seriously raises the risk SMBs are exposing themselves to without the proper IT infrastructure in place.

In reality, SOX really should not even be viewed as just a government mandate. The fact is SOX is already the de facto standard for many industries and businesses and the law's requirements simply make good business sense as it puts controls and processes in place that generate efficiency, effectiveness and greater performance.

There have already been several extensions granted by the government for SOX compliance, but I do not recommend that small public companies regard this as a reason to delay implementing the process. Instead they should use the time to improve their compliance process including documentation and if possible, spread the costs over multiple years. The compliance and security tasks can be quite challenging for the SMB that most likely does not have internal IT resources, therefore seeking external help. Many will need all the time left to comply.

In order to remedy security problems, a company must first develop a security plan and integrate it with IT policies. Once these policies are created they must be maintained and monitored so they remain active and effective, keeping those involved on the same page. Security needs should be focused on all levels, not just on the database and applications. Also, each aspect of compliance should be tackled one at a time. Each one will have different requirements and concentrating on them separately will minimize confusion and will enable a business to complete the task safely and efficiently.

Once a company takes the time to invest in IT security, they will see the benefits it can bring to their business that go beyond compliance. It is important for management to integrate technology into the overall corporate plan. First and foremost, it is to ensure that both business strategy and the IT strategy are in sync. This is the best way to ensure that the company derives the best return on investment on their IT assets. Secondly, IT provides the platform to be able to build a standardized, integrated, best-of-breed, sustainable business process that all authorized employees can utilize. This will lead to better risk management, increased productivity, improved revenues, reduced errors, controlled costs, and so on.

Compliance and security challenges can be extra daunting for the average SMB, which is most likely facing daily pressures to keep customers satisfied, increase revenue, and make cutbacks to save money. However, once it is complete, they will enjoy the many benefits.

Overall, the risk level for the organization will be reduced and the business will now have documented policies and procedures to follow. IT processes and controls will now be documented. The business will see a significant cost savings for the organization now that controls are automated as opposed to relying on manual controls and focusing on preventive rather than detective controls. The design of key controls of lower frequency (for e.g., monthly controls as against daily controls, etc.) will also help significantly in reducing time and costs for achieving compliance. The business can also expect significant deficiencies and material weaknesses to be reduced if not completely eliminated as a result.

Independent surveys have shown that firms that are compliant report up to 13 percent better valuation. It will also enable the business to have greater ability to carry out merger and acquisition transactions with listed companies, not to mention it will be even easier to conduct business with customers and vendors.

Last but not least, companies will embrace the many benefits of security compliance. Compliance will protect the business from external users hacking into their IT infrastructure including databases. SMBs must be protected against threats such as password stealing as well as security vulnerabilities such as SQL injection, which is present when user input is either not filtered correctly or not strongly typed and thereby unexpectedly executed, or brute force, a method of defeating a cryptographic scheme. On the internal end, weak passwords will have to be eliminated and data will have to be password protected to which only authorized users would have access to. Security compliance will also have to eliminate any chance of web and application servers from data and audit log tampering. Better protection of system backups will have to be implemented.

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 is about integrating policies and procedures as well as an overall structure that protects an enterprise, its assets and performance.

Sumit K. Pal is the Executive Vice President, Operations, of [WithumSmith](http://www.withumsmith.com)+Brown Global Assurance, www.wsbga.com.