



Information Your Greatest Asset

How Vulnerable Businesses Can Protect Information Assets While Improving Security, Compliance and Productivity

Whether you are the manager of a bank or the owner of a small franchise sandwich shop, no business leader in their right mind would leave the keys to the safe open and the door unlocked after hours. That's because protecting assets is a shared top priority among all business types and sizes. However, for many small- and mid-sized businesses, an often overlooked asset that's typically not adequately protected or utilized is information. Everything from vital paper records in human resources to vendor invoices in accounts payable or electronic or paper versions of data should be considered informational assets and therefore protected. And, what few SMBs are aware of is how vulnerable their businesses are if they don't adequately protect and secure their greatest asset.

In this paper, we will detail the following to help SMBs become less vulnerable, more secure and achieve higher levels of productivity and profits:

- >> the common ground among SMBs' shared departments and factors threatening their informational assets
- >> the top motivators for why SMBs should do more to protect their information
- >> how businesses can better secure and manage their information

Threats from the Physical & Non-Physical Worlds: Leading Factors Causing SMBs' Loss and Misuse of Information

An organization of any type that processes information, whether educational, financial or non-profit, will handle the responsibilities of departments like human resources, accounts payable/receivable and customer records, to name a few. The threat factors for these departments' information are also common denominators. Information - whether paper files or electronic data stored on servers - can be threatened by the exchange of information between customers or employees on unsecured Internet connections; targeted hackers and computer viruses; power black-outs and natural disasters, as well as access of the information by unauthorized users. As the number of "virtual employees" among businesses grows, additional threats face the company of "mobile workers" when information on individual laptops, PDAs and cell phones is not protected by one universal company plan or system.

Protecting information assets is a shared top priority among all business types and sizes.

KEY TAKEAWAY

SMBs across all industries are equally vulnerable when the information vital to running their operations is at risk from being insecurely accessed, destroyed by physical or virtual disaster and non-uniform guidelines for mobile employees. And, beyond increasing vulnerability, misuse of information ultimately costs businesses their profits by negatively impacting productivity.

Businesses may be acutely aware of stories like the loss of information experienced as a result of the catastrophic events of Hurricane Katrina on New Orleans. However, they fail to recognize the factors in their own backyard such as how their electronic records are vulnerable if IT systems are not adequately protected against online threats or how much information their systems back up if there's a sudden power outage. And, regardless of what hurricane zone your business is physically in, if you store any type of paper documents, you're also at risk and in some cases not compliant if those documents are in harm's way (i.e. fire, flooding, or other physical destruction causes).

Final Four's of Information Management: Security, Compliance, Business Continuity and Productivity

Step one in better information management is to recognize the key threats to your business' informational assets and take steps to guard against such causes. The top four motivators essential to why businesses should and need to implement an information management plan are security, compliance, business continuity and productivity.

Security

Security is among one of the top priorities for protecting information as an important asset. An effective information management system should account for the secure exchange of information within a company's network or via the Internet and the accessing of information only by authorized users (as arranged by security levels for different departments or employees). Additionally, information should be managed so that any original hard copies of important documents are backed up with electronic copies on an off-site server in case the paper versions are physically lost, stolen or destroyed.

Security is a key motivator as businesses with customer information of any kind are susceptible to issues including identity and information theft, breach of information for competitive risks, or complete loss of information from a natural disaster. Companies that suffer information loss also lose their ability to operate their business.

Compliance

Compliance goes hand in hand with security. Companies that have unsecured information are often not in compliance with government, industry or business standards and requirements. These can vary by industry, with HIPPA affecting healthcare, Sarbanes-Oxley affecting financial services and industry or parent-company regulations often affecting franchisees, but nearly every company is required to be compliant with more than one regulation. And, one that obviously affects every business is the IRS and tax audits. In light of corporate accounting scandals of recent years, an information management system should also address records management plans with automated vs. manually driven policies.

The best way to be prepared for compliance standards is for a business to regulate itself. In today's lean, competitive business environment, the only way to do that efficiently is with an information management process and solution that manages internal audits, monitors employee's workflow and provides secure and immediate access of records to the appropriate members of an organization. Any SMB that plans to eventually be acquired or sold as a phase-out plan (whether an owner's retiring or wanting to grow into a partnership with like organizations) must prove to potential buyers that they are regulated, monitored and accountable for their practices, much like larger corporations. In order to comply, they need a technology system that makes internal audits and information monitoring affordable, timely and efficient. Non-compliance for any business that wants to be sold is a huge liability factor to potential buyers.

Business Continuity

Many SMBs buy disaster recovery solutions out of fear. However, they face a negative return-on-investment (ROI) if the solution only addresses the 'what-if' scenario - the one in a thousand chance that disaster will hit - instead of incorporating an end-to-end strategy on how business will steadily continue regardless of the interruption, whether it be a large disaster or a factor as seemingly insignificant as a key employee being sick or the relocation of an office.

To address disaster recovery as part of an overall umbrella plan for business continuity with an electronic information management plan, SMBs can lessen their reliance on paper-driven processes, which is often the cause of disasters that afflict businesses.

According to independent market research commissioned by Veritas, although 96 percent of companies have at least one solution to help them get their technology infrastructure back up and running, 92 percent polled believe there would be serious consequences if they actually had to implement their disaster recovery plan. And 57 percent of companies with a disaster recovery plan do not address business continuity, the performing of daily functions necessary to keep a business afloat. This differs from IT strategy in that it involves much more than bringing up a computer system and applications.

To address disaster recovery as part of an overall umbrella plan for business continuity with an electronic information management plan, SMBs can lessen their reliance on paper-driven processes, which is often the cause of disasters that afflict businesses. When a storm hits, or an employee leaves who was solely responsible for knowing how paper files were stored and organized, it's the employees' reliance on those physical factors that causes the interruption in the business' continuity.

Productivity

Business owners, being inherently human, are driven by fear. Factors like security, compliance and preparing for a disaster with continuity plans are motivation enough for SMBs to improve their information management plans. The extra-credit bonus that comes with being secure, compliant and continuous in business plans is that as a result of those process and technology improvements, companies are ultimately more efficient, productive and profitable.

The main productivity benefits are readily apparent - information that is available electronically in one centrally organized system is more easily accessed and organized than when it is stored in separate silos (from filing cabinets to different file formats and computer desktop folders). Information that is systematically regulated by an automated records management policy that retains data for a specified amount of time and purges the system of it, saves the time, effort and potential human errors of employees who have to file, look up and handle information with paper-driven processes and schedules.

And, organizations with long-term continuity plans in place ahead of time naturally operate more efficiently in day to day business. When it comes to having to meet compliance or security standards, being productive with an effective information management system and processes can make audits from the IRS to industry monitoring much more efficient, saving employee time and money and ultimately helping the business to run better.

The How Behind the 'Why': What an Effective Information Management Solution Entails, and How to Practice It

Many SMBs are baffled by the sheer number of technology solutions available to aid them in every facet of their business. There are, for example, specific solutions for records storage, accounting or compliance regulations by industry. The biggest investment mistake many SMBs make, however, is choosing an expensive solution that only solves one facet of their business problems, instead of optimizing an end-to-end solution that enables organizations to easily and strategically create relationships between important, disparate pieces of information.

Many existing solutions also fail to recognize or leverage informational relationships within an organization. Effective solutions are ones that bridge the gap between digital content and paper documents and help organizations intelligently link and match documents to important data objects such as people, companies, processes and assets. Besides being a solution that will benefit more than one aspect of an SMB, technology for the mid-market should also be affordable and scalable according to the needs of each organization's size, industry and individual needs.

The real ROI of such a solution is that it will help SMBs address key business issues beyond compliance. Its effects are seen across the business from improving communications to enhancing customer service and providing immediate access to information and relationships within the data to all system users.

The biggest investment mistake many SMBs make is choosing an expensive solution that only solves one facet of their business problems, instead of optimizing an end-to-end solution that enables organizations to easily and strategically create relationships between important, disparate pieces of information.

Nuts & Bolts: Components of Security, Compliance & Productivity Solutions

Solutions that effectively deliver that type of ROI typically integrate components of document management, information management, document imaging, workflow management and relationship management. These types of components working together should turn data into usable information. In layman's terms, the data and records employees once sought in the documents filed away in cabinets or images scanned onto a hard drive are now immediately available, searchable and secure.

An effective system should also manage the relationships within the data. Meaning that a particular record, for example, should obviously correspond with other relevant pieces of data like a customer's account, business, purchase history, etc., when users are looking up that piece of information.

SMBs shopping for an effective solution to protect informational assets, meet security needs and compliance standards and improve productivity should look for a product that includes the following defined components:

>> **Document Management** - An intuitive interface that automates the management of documents and their versioning, auditing and archiving. Annotations, color-coded document status and multiple levels of security are ideal features in a management module.

>> **Imaging Management** - Input management that captures multiple documents makes the job of document preparation and scanning easier.

>> **Workflow Management** - Automates and monitors internal procedures, allowing critical path processes to be assigned to documents. With user-definable fields and flexible options, workflows should be easily configured for existing processes and provide improved and efficient task management along with multiple levels of accountability and control.

>> **Search** - Instant access to information through multiple search tools for documents, content, relationships and data. Documents can be quickly and easily found through user-defined key words and criteria or through full-text search.

>> **Non-Custom Application Integrator** - Users should be able to pull data from another application without the expense of custom integration. This data can be used to search for a document, index a document or populate and search the relationship manager, the time consuming task of data entry.

By recognizing the common risks and motivations SMBs share, and selecting a solution that enhances work process while improving security, compliance, continuity and productivity, companies across the mid-market (and regardless of industry) are on their way to protecting their informational assets with as much guarding as they would the cash in their safe.

About FileVision

FileVision is a global software company that develops information relationship management software. Our solution, FileVision, empowers organizations to bridge the gap between digital content and paper documents by intelligently linking and matching documents and information to important data objects such as people, companies, processes and assets. Government, healthcare and financial services organizations worldwide rely on our technology to help them improve communications, enhance customer service and immediately access information and relationships within data. FileVision is headquartered in Atlanta, GA with offices in the UK, Australia and New Zealand. For more information, please visit www.filevision.com.

CONCLUSION

By recognizing the common risks and motivations SMBs share, and selecting a solution that enhances work process while improving security, compliance, continuity and productivity, mid-market companies (regardless of industry) are on their way to protecting their informational assets with as much guarding as they would cash in their safe.