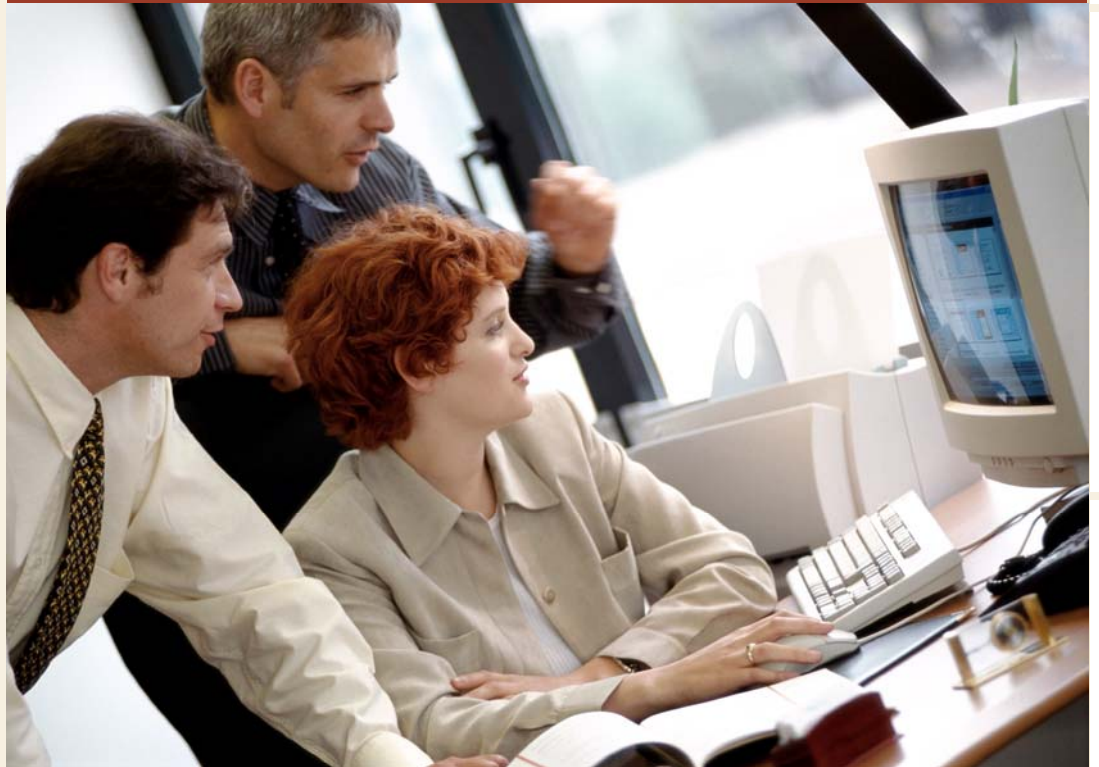


Business Value of Reducing Costs and Risks of e-Discovery and Regulatory Compliance



4080 McGinnis Ferry
Road
Suite 603
Alpharetta, GA 30005
www.ebstrategy.com

Sponsored by



Copyright © 2006

www.ebstrategy.com

Table of Contents

Executive Summary	3
Business Drivers Impacting e-Discovery and Regulatory Compliance.....	4
Business and IT Management Implication	5
Technology Challenge: Archiving E-mail and Messaging.....	6
Archiving and Discovery Solution Requirements	7
Retrieval	8
Solution Planning and Evolution.....	9
The Enterprise Vault Solution.....	9
Business Value of Enterprise Vault	11
Customer Success with Enterprise Vault.....	12
Webcor Builders	12
Advantage Sales and Marketing LLC	13
Symantec Corporation	14
Conclusion.....	16

E-Business Strategies, Inc.

E-Business Strategies (ebs) is a technology research and ROI consulting practice. The company offers cutting-edge research, customized consulting services, white papers and innovative educational programs. E-Business Strategies' services are designed to give companies the ability to sense, adapt, and respond quickly to changes in the marketplace.

Executive Summary

Business Need: Recent trends in statutory law and business litigation elevate the stewardship of business data archives—particularly e-mail and messaging data—to a high priority for information technology managers.

Failure to maintain “on-demand” access to relevant business information for regulators can lead to significant financial penalties or serious weakening of an organization’s legal position during legal disputes. Furthermore, the cost of executing searches of poorly organized archival information can generate significant IT department workloads that add expense to IT operations, create unnecessary risks to the enterprise, and detract from higher value-added activities.

Solution: The e-mail and messaging archiving solution from Symantec based on Veritas Enterprise Vault represents a comprehensive approach to archiving, storing, and retrieving electronic business records. Main functions enabled by Enterprise Vault include:

- Automated, ongoing capture of relevant data from e-mail, file, and other electronic content sources—particularly important in the context of applying “legal holds”
- Ability to migrate data to lower cost, long-term storage and reduce duplication of data
- Indexing of archived data to facilitate efficient searches at a later date
- Discovery, capture, and indexing of existing client-side e-mail archives (.PST files in Microsoft Outlook)
- Ability to set and execute policies to manage the data capture, retention, and destruction lifecycle
- Differentiated sets of user interfaces and access controls for multiple classes of employees, from rank-and-file desktop users to the legal department to IT department “super-users”

- Consolidated management of e-mail and messaging storage across an organization

Benefits: The areas of business value of a consolidated approach to data archiving and retrieval include:

- Reduced risk and cost of archival capture, searches, and production for litigation support and internal investigations (e.g., contract disputes, HR claims, intellectual capital infringement, etc.)
- Lower risk of regulatory non-compliance for information retention, monitoring, and supervision (e.g., SEC 17a-4, NASD 3010, HIPPA, etc.)
- Lower risks of data gaps and deletions resulting from inadvertent deletions or storage of messaging data on mobile or unconnected platforms (i.e., enabling “legal holds” across an enterprise including laptop computers, PDAs, messaging cell phones, Blackberry devices, etc.)
- Ability to migrate data to price-performance, optimized long-term storage
- Ability to migrate data multiple times over its lifecycle to the most cost-effective storage as technologies and storage economics inevitably change
- Use of data compression and single-instancing technologies to reduce the footprint and duplication of archived data
- Decreased cost of consolidated administration of messaging storage, compared to self-administration of e-mail storage by individual employees

Business Drivers Impacting e-Discovery and Regulatory Compliance

Over the past several years, a new wave of legal precedents and government regulations added a new business-critical responsibility to enterprise information technology (IT) programs. Governments and the legal system now require extraordinary visibility into information used by private and public sector organizations to run their operations.

In addition to coping with a steady level of government oversight and reporting, the legal system can generate unpredictable and far-reaching requests for information that must be satisfied quickly and completely. Particularly in the U.S., litigation has become a routine business management function on par with other traditional business functions such as Finance, Sales, and Operations. Many companies now continually manage a portfolio of legal actions ranging from human resources claims and contract disputes to major antitrust, liability, intellectual property, and corporate governance lawsuits.

In the U.S., legislation such as the Sarbanes-Oxley act, the USA Patriot Act, and other laws—plus

regulatory initiatives by the Securities Exchange Commission (SEC), National Association of Security Dealers (NASD), state governments, and others—have placed a regulatory spotlight on what were previously private communications and recordkeeping. Worldwide, actions such as the Basel II accords, the United Kingdom Financial Services act, and the European Union Model Requirements for the Management of Electronic Records (MoReq) have had a similar effect on organizations conducting business in these jurisdictions.

Depending upon where they conduct business, companies can face complex patchworks of regulatory requirements. They may need to be prepared to meet regulatory requirements of every country or legal jurisdiction in which they operate—even when local laws conflict, overlap, or create ambiguity. Furthermore, many U.S. state governments have significantly different and more rigorous corporate governance and business regulations than the federal government. Some state regulations, such as California’s SB 1386 data privacy legislation, apply to companies transacting business with customers residing in the state, even though the company may have no offices or business presence in California.

Regulatory requirements also vary according to what business an organization pursues. Publicly traded

	SEC 17a	NASD 3010	HIPAA	21 CFR 11	Sarbanes Oxley	California SB 1386
Public Sector			⊗			
Public Companies	⊗		⊗		⊗	⊗
Financial Services	⊗	⊗	⊗		⊗	⊗
Healthcare			⊗		⊗	⊗
Life Sciences			⊗	⊗	⊗	⊗
Other			⊗		⊗	⊗

Figure 1: Different types of organizations may be subject to different sources of regulatory exposure.

companies in the U.S. may be subject to Sarbanes-Oxley, SEC, stock exchange (NASDAQ, NYSE), and financial, accounting, or auditing standards. Financial services firms, healthcare organizations and, others face additional specialized regulatory information disclosure requirements. Even governments and non-profit organizations may need to observe laws and regulations that apply to public sector organizations.

Data retention and archiving requirements vary widely, depending upon the laws or regulatory bodies that govern them. For example, the NASD and the SEC require broker dealers to retain client transaction records for six years, while the U.S. Occupational Safety and Health Act (OSHA) requires that certain types of information must be retained for 30 years. The Health Insurance Portability and Accountability Act (HIPAA) calls for retaining patient information for the lifetime of the patient, plus six years. In addition, Sarbanes-Oxley stiffens enforcement of retention requirements that already exist in other legislation and regulations.

Business and IT Management Implications

The far-reaching demands for public access to information from governments and the legal system puts tremendous pressure on IT departments. Today, almost all written communications generated by an organization is processed and recorded on computer systems of various kinds. This has made information contained in IT infrastructures, such as its databases or e-mail

archives, an important resource for lawyers, regulators, and financial auditors seeking information on an organization's most intimate operations and decision making.

At the highest level, discovery and compliance are primarily a cost-of-doing-business issue, involving the expense of retaining and retrieving data for purposes unrelated to an organization's primary value-generation mission. More indirectly, they can also reduce money available for higher return-on-investment business initiatives.

Discovery and compliance costs involve both proactive and reactive elements. Proactive costs include those stemming from storing data and maintaining access to it for required periodic reporting and audits. These costs are largely predictable and therefore easy to forecast and budget on an annual or multiyear basis. Reactive costs come from responding to requests to supply data for litigation or other discovery requests. Because these types of requests are unpredictable in terms of their frequency, scope, gravity, and required detail, they are more difficult to anticipate.

Costs can spiral out of control if retention and discovery are performed incompletely or ineptly. In the U.S., there have been

cases where litigation-related discovery requests resulted in hundreds of thousands of dollars or even millions of dollars in fees for computer consultants hired to find relevant information in sub-optimally maintained archives. Incomplete or haphazard response to information requests may even violate regulatory requirements and/or generate the

Important legal concepts associated with e-Discovery

- **Legal Hold or Litigation Hold:** Companies are required to retain data that might be subject to e-Discovery—even prior to the court matter officially started. Because of this, companies are forced to “suspend destruction” of information that might be involved in the case. This often comes in the form of a list of users whose e-mail needs to be retained or a list of keywords that need to be maintained. Today, companies do this in very suspect ways like suspending recycling of all backup tapes (even if only a few users e-mail is to be retained) or e-mailing users asking them to manually retain information that is “on hold.”
- **Chain of Custody:** Throughout the entire process of collecting, processing, and producing information for evidence, companies are required to show that the evidence maintained a consistent “chain of custody” where it was not tampered with or altered in anyway. With the number of manual steps in typical e-Discovery processes today, this is very difficult to claim.

impression that an organization is tampering with or suppressing information. This can weaken an organization’s legal position, result in financial penalties, or even turn a civil matter into a criminal one.

In addition, poorly designed information management systems may create obstacles to compliance in the event a subpoena or document requests appears on the doorstep—with the risk of inadvertent destruction triggering astronomical sanctions and potential criminal liability, organizations must design their IT systems with “legal hold” capabilities in mind. It is important to put a legal hold or “lock down” data that becomes responsive to a regulatory matter, investigation or subpoena. Most of the case law is driven by companies that fail to do this or allow others in the organization to delete data. Companies must use the same level of diligence with their technology to support legal holds that they use with their production business environment. For example, if there is rotating of tapes and they have active litigation or investigation, what steps are they taking to preserve potentially responsive information—is there an infrastructure to lock down information on laptops and servers?

Discovery and compliance costs and risks can be lowered through prudent planning, deployment of cost-saving technologies, and execution of operational best practices. While the main internal customers for IT-supported compliance and discovery services—usually lawyers, finance people, and senior management—will define policies and set service level requirements, the IT department plays a crucial role in delivering an archiving and retrieval solution to meet service level requirements at the lowest possible cost.

Technology Challenge: Archiving E-mail and Messaging

E-mail and messaging data have emerged as a primary concern for IT departments coping with discovery and compliance. The volume of e-mail and messaging data is exploding, creating enormous demand for archival storage. E-mail has become a business-critical application with four out of five enterprises using e-mail to conduct business transactions. The average messaging user sends and receives nearly 25,000 e-mails annually; and this

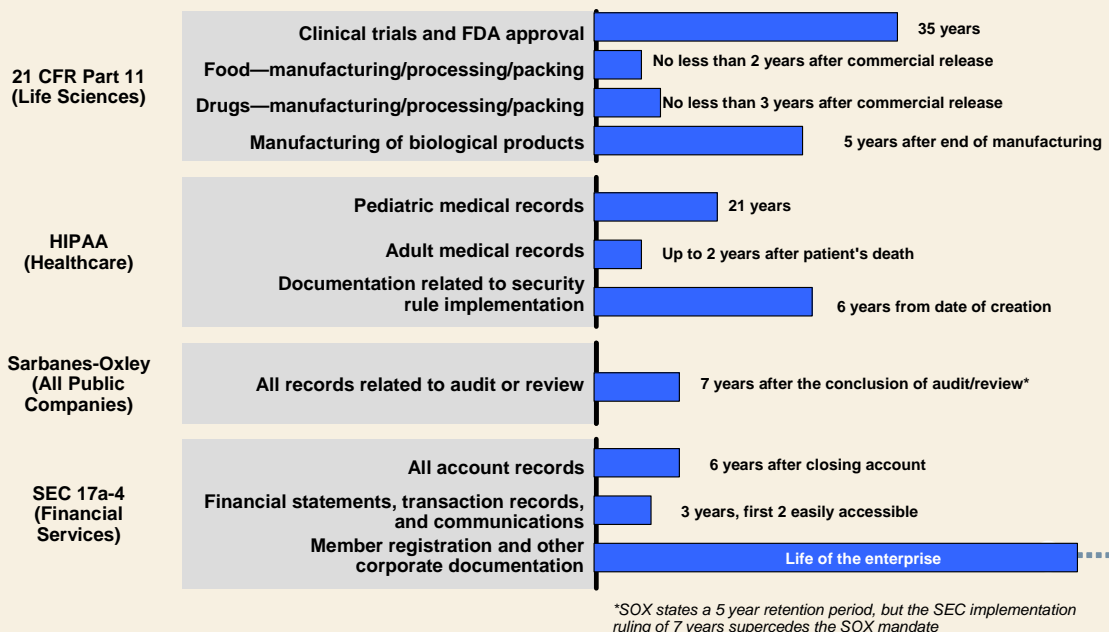


Figure 2: Regulations Drive Retention and Discovery

number will continue to grow. The consequence to this large and growing volume of e-mail is that e-mail is being increasingly used for legal discovery.

E-mail content has also become richer in terms of storage and bandwidth requirements; they are no longer plain text, but often embed formatting and graphics information. E-mail also frequently includes attached documents that may require megabytes of additional storage. Consequently the e-mail system has become a virtual file system containing a wide range of information.

The popularity and casualness of e-mail can be a source of regulatory and discovery risk. It's all too easy for employees to relax and document indiscreet thoughts and actions that may later prove damaging to a company's interests. It is little wonder that e-mail files have emerged as an important resource for lawyers and regulators seeking to learn about "what was really going on" inside an organization.

Archiving and Discovery Solution Requirements

Archiving and discovery solutions encompass four areas of activity:

- Retention
- Retrieval
- Lifecycle Management
- Solution Planning and Evolution

Retention

Data retention involves decisions about which data to archive and what resources to use to store it. When it comes to e-mail, some believe the best default choice is to plan on storing all e-mail, instant messages, and attachments—even spam—as it is

impossible to foresee what might become relevant to a regulator, lawyer, or manager at a later date. Here, the main concerns are the ability to capture all relevant data, storing it economically and in a state ready for easy retrieval when necessary.

There are about 686 million e-mail users worldwide, with over 1.2 billion active e-mail accounts. Worldwide e-mail traffic per day totals about 141 billion messages.

The Radicati Group, "Q4 2005 Market Numbers Update," January 4, 2006

Archiving data usually begins with moving it from primary storage to less expensive storage resources. The archive must also be secure from all points of view—environmental, physical,

user privilege, and network/remote access. Transfers of data from one medium or platform to another must also take place flawlessly. This is important, as archived data may migrate to several different platforms over its lifecycle when technologies and quality-of-service requirements change.

Archives can be huge, storing millions or even billions of e-mails, attachments, messages, and other data. Archiving also presents an opportunity to economize on storage resource requirements through data compression and single instancing of duplicate data. Data eligible for single instancing can include e-mails and attachments sent to multiple addressees. It is also important that even as data may be compressed or single-instanced in the archiving process, there can be no question that data has become distorted, corrupted, or deleted.

IT managers should also be concerned about archiving dispersed data that may not always be visible to, or captured by, centralized resources. This includes data on employee laptop computers, mobile, and remote access systems. This concern will likely increase in urgency over the next several years as more regulatory- and discovery-sensitive messaging data is carried on cell phones, PDAs, memory cards, flash drives, and even consumer devices such as multimedia players.

Many organizations have attempted to cope with the e-mail data explosion by setting user storage limits. This can be counterproductive when it

comes to compliance and discovery archiving. Instead of consistent retention policies, instituting storage limits turns employees into their own data archiving manager. Not only does this waste employee time, an organization may find it has as many data retention policies as it does employees—as well as disparate locations to access (such as employee laptops) in the event of a discovery request. This can lead to expensive, frustrating searches and even expose an organization to accusations of manipulating or suppressing information.

65% of organizations consider growth in messaging storage to be a serious or very serious problem, slightly more problematic than the problem of spam itself.

Osterman Research, “Messaging Security Market Trends, 2005-2008,” May, 2005

Retrieval

From a retrieval point of view, e-mail qualifies as unstructured data, making it difficult and expensive to find proverbial needles in haystacks as is often required in information discovery actions. To enable efficient searches at a later date, information contained in e-mail should be indexed as it is archived. Search criteria can take seemingly infinite forms and include key words from metadata (addresses, transmission time and date, etc.), message body content, or attachments. This also means that the archiving solution should be able to retrieve information from multiple data and document formats.

Conventional backup and disaster recovery technologies and processes are not optimized to enable precise location of specific pieces of information that may be buried in terabytes of e-mail archives. These technologies are designed to restore the status of an infrastructure as a whole, not find specific pieces of information it may contain. Further, a standard cycle of daily, weekly, or monthly disaster recovery backups delivers a snapshot of data active on an infrastructure at the moment the backup occurs. A lot of regulatory, or discovery-sensitive business, may take place between backups, running the risk of the incomplete capture of such data, which may be needed for retrieval at a later date.

Personnel accessing the archive can include rank-and-file end users, company management, corporate

and outside counsel, regulators, and investigators. Search capabilities, service levels, and ease-of-use requirements may vary among classes of end users. An employee treating the archive as a transparent extension of their home directory, for example, will probably want a simpler user experience than a legal team seeking to reconstruct communications among a group of executives over a period that may stretch back several years.

Archive managers also face a dilemma between enabling access to archived data and ensuring privacy and confidentiality of certain classes of data. This means that appropriate access controls and policies must be built into the archiving solution.

Finally, archived data should be converted into an obsolescence-resistant (“future-proof”) format such as HTML. In the event that the application that created a given document is no longer available (e.g., an older version of Microsoft office), it is still critical that the organization is able to read the relevant information. Although HTML rates as the current preferred method for storing data, solution managers should remain alert to unanticipated technology changes that could supersede this choice.

Lifecycle Management

Managing information lifecycles involves setting and executing policies for retention, migration, and eventual disposition for various classes of data. As noted earlier, different laws and regulations specify varying policies for the types of data that must be retained and how long it must be kept. Rules can even vary depending upon the employees in contact with the data within an organization. For example, data relevant to senior management, the board of directors, or others with governance and fiduciary responsibilities may need to be handled differently than that of rank-and-file employees and middle managers.

It is particularly important that lifecycle policies be consistent, clearly stated, and promptly executed. It is quite defensible to tell an inquiring attorney or regulator that data has been deleted according to

policy if that policy conforms to prevailing laws and regulations and applied uniformly. Retention policies that are ambiguous or executed inconsistently open the door to suspicions of tampering with data.

Solution Planning and Evolution

Planning a solution and evolving it as business requirements and technologies change provides the ability to create and execute data archiving and discovery solutions that meet specific organizational situations and requirements. Variables include the business the organization pursues; prevailing laws and regulations in the regions in which it operates; and the overall scale of archiving and discovery requirements. Organizations should also plan for growth in the scale of the archiving operation to accommodate the expansion of overall business operations, increasing deployment of e-business processes and growing richness of content subject to archiving.

The archiving solution should also be storage-platform independent with archived data eligible for storage on a wide variety of physical (disk, optical, tape), software, and virtualized (NAS, SAN, etc.) resources. This also includes decision making about whether to maintain the

archiving and discovery solution in-house or to outsource it.

The Enterprise Vault Solution

Veritas Enterprise Vault archiving and discovery software from Symantec Corporation enables and supports long-term archival storage and efficient retrieval of unstructured data, especially Microsoft Exchange-managed e-mail, instant messages, and attached documents. The application offers similar services for Lotus Domino-based (journal) e-mail and messages. Main capabilities of the software include:

- Ability to set rules and policies for retention lifecycles—i.e., what to store, where to store it, how long to keep it, what to do with it after an expiration date.
- Indexing information within unstructured data to facilitate later, Boolean search-driven retrieval.

Enterprise Vault Archiving Framework

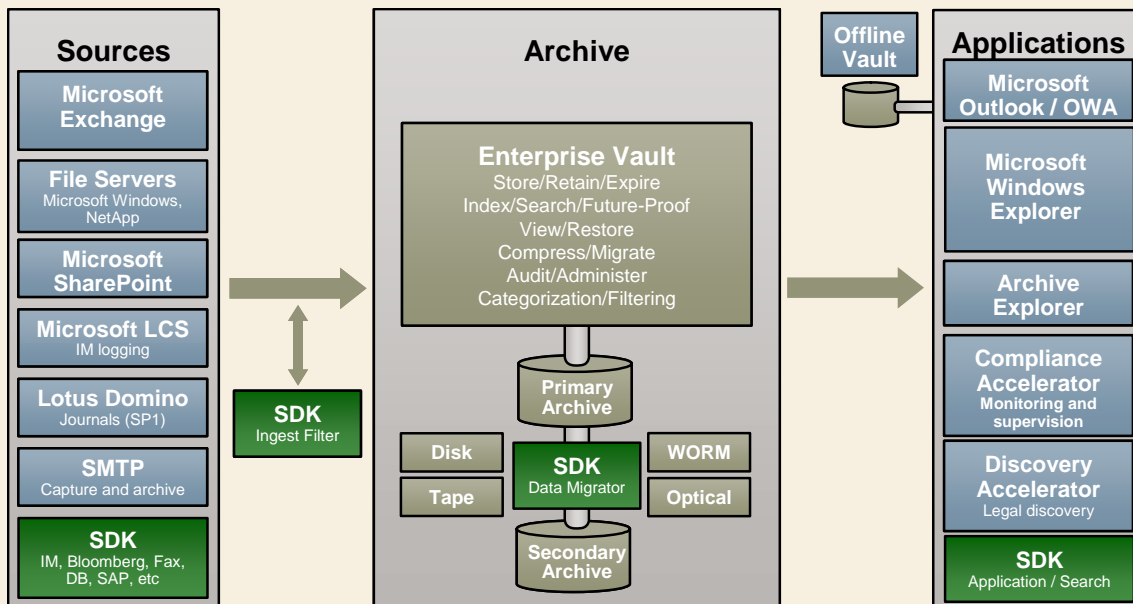


Figure 3: Enterprise Vault Archiving

- Enabling rapid searching, and production of archived information for discovery purposes.
- Centralized administration console (Microsoft Management Console plug-in) to define policies and user privilege and access controls.
- Graphical user interface for access to archived information; integrated with Microsoft Outlook and Microsoft Windows Explorer.

The Enterprise Vault Archiving Framework, as illustrated in Figure 3, consists of a three layers:

- **Sources.** This layer provides archiving services for application-specific data generated by Microsoft Exchange Server, Microsoft Share Point Portal Server, Lotus Notes/Domino, and generic SMTP mail systems. The layer also provides an interface to enable development of customized archiving solutions for a wide variety of content.
- **Archive.** The modules at this layer provide working-level archiving, content indexing, compression/instancing, retention, security, and policy execution services as defined and prescribed by solution administrators and managers. Enterprise Vault supports archiving on a wide variety of storage media and architectures, including disk, tape, optical, storage area networks (SAN), network attached storage (NAS), and content addressed storage (CAS.) A key feature of this layer is the ability to archive data on the most cost-effective platform and to keep datacenter availability roadmap options open to expeditiously migrate data to different platforms as technologies, user business requirements, and storage economics evolve.
- **Applications.** This layer provides users and management with an interface to services available through the Enterprise Vault solution. It enables end users to interact with the archive as a natural extension of their use of familiar desktop applications such as Microsoft Outlook, Microsoft Windows Explorer, or various Web browser (Microsoft Internet Explorer, Netscape, Firefox, etc.).

Some Successful Enterprise Vault Deployments

- **Q Associates**, one of the leading technical computing specialist firms in the U.K., leverages Veritas Enterprise Vault from Symantec to reduce the size of its Microsoft Exchange mailboxes by nearly 60% and e-mail maintenance windows by nearly 80%.
- **Direct Media Inc.**, a leading direct marketing firm, implemented an e-mail security and availability solution from Symantec, including Veritas Enterprise Vault and Symantec Mail Security, to avoid \$60,000 in additional e-mail server and storage costs and to reduce the number of file servers from six to one, with a resulting tangible total cost of ownership.
- **Somerfield Stores, Ltd.**, archived four million e-mail messages over a period of 18 months using Veritas Enterprise Vault from Symantec. The e-mail management solution allowed Somerfield to reduce e-mail storage requirements by 30% while reducing e-mail storage growth by 50%.
- **Broadcast Australia**, the leading independent broadcast transmission provider, reduced its e-mail storage volume by 85% and will save a projected AU\$75,000 over a three-year period using Veritas Enterprise Vault software.

Management access takes place via the Microsoft Management Console. The software includes Enterprise Vault-specific tools and “wizards” to enable fast configuration of enterprise-specific solutions. Access services can be configured to enable remote admission to the archive for mobile users and establish user privilege controls. The Universal Shortcuts feature enables users to set up pointers to frequently used folders and individual messages in the vault. These act much like familiar Microsoft Windows Explorer shortcuts and can be used to point to Microsoft Outlook and other documents. Business Accelerators help automate workflows associated with archive searches conducted for regulatory compliance or legal discovery actions. The accelerators help organize a

search in advance and can be stored for later use in follow-up actions and reporting, or for performing due diligence for the periodic reporting and disclosure associated with such mandatory filings as quarterly earnings reports or SEC statements.

Enterprise Vault follows a building-block approach focused on providing maximum scalability. Medium-to-large enterprises are optimal candidates for this robust application. It has also been deployed successfully and generated value at smaller organizations such as law firms, accounting services organizations, financial institutions, and other enterprises with high exposure to legal discovery risks and government regulation. In terms of maximum capacity, Symantec and partners have qualified Enterprise Vault for implementations serving up to 100,000 end-users and foresee no reason to prevent building even larger installations.

Business Value of Enterprise Vault

Based on research from Enterprise Vault customer experiences and internal sources at Symantec, E-Business Strategies ascertains that Enterprise Vault generates benefits in five areas related to cost savings, cost avoidance, risk reduction, and business process productivity improvements:

- **Reduced cost of responding to legal and regulatory inquiries.** In the absence of a dedicated e-mail archiving solution, responding to litigation- or compliance-generated e-mail archive inquiries may require as much as 50 to 100 hours of IT staff time per inquiry. For an organization responding to even as few as 25 inquiries per year—roughly one every two weeks—this non-revenue generating activity can become the equivalent of a full-time position. A properly configured, well-maintained Enterprise Vault solution may reduce inquiry response turnaround times to as little as one hour. Even if one-hour response times represent an extreme case, it is reasonable to expect a 90% response time reduction (from 50 hours to five hours, or from 100 to 10 hours), with tangible resulting IT labor savings.

- **Reduced risk of penalties and weakened legal position.** Implementing an e-mail management solution based on Enterprise Vault offers a high assurance of capturing all regulatory and legally sensitive e-mail information, which reduces vulnerabilities to non-compliance fines and penalties. But because every organization faces a unique regulatory environment—and because it is inherently difficult to predict what kinds of legal actions may be lodged against an organization, their resulting economic consequences, or even the attitude of regulators to a given company—it is difficult to quantify savings in this area. The only accurate measurement of risk reduction benefits would be for organizations to compare their yearly total fines paid for inadequate disclosure before and after implementation of an Enterprise Vault archiving solution.

Inadequate record keeping can also undermine an organization's legal position during litigation and other claims actions. It can reduce the amount of positive evidence a company may have available to support its interests in a legal action. Specifically, the inability to provide evidence requested in a subpoena or other discovery action may generate specific fines and penalties or create a presumption that an organization is hiding or tampering with evidence. Also, a suboptimal archiving solution may create incentives for organizations to settle cases—which, strictly speaking, they otherwise would have won—in order to avoid the high costs of retrieval. For example, a plaintiff may seek damages of \$150,000 from a company on a weak case knowing that document discovery and attorney fees will cost the defendant at least that amount of money if the case goes to trial. Consequently, it makes business sense to settle the case in the plaintiff's favor to avoid discovery-phase costs, even though the defendant's counsel may believe their legal position will ultimately prevail.

- **Reduced cost of archival storage.** A dedicated archiving solution creates opportunities to move data to less expensive storage resources and to continue migration of the data to progressively

lower-cost storage as technologies evolve over the years. Also, data compression and single-instancing technologies offered by Enterprise Vault work to reduce archival storage space requirements for archived data. Typical organizations experience an enterprise-wide single-instance ratio of 1.3. Couple this with the ability of Enterprise Vault to achieve 20% or more message compression, and the result is a reduction in archival storage that produces a decreased archival storage cost.

- **Reduced cost of e-mail account administration.** The opportunity to centralize e-mail account administration can offer savings by relieving employees of this job function. Research indicates that employees may spend an average of one hour a week administering their e-mail accounts to stay within organizationally mandated storage limits. It is easy to see that multiplying one hour a week by 52 weeks by the number of employees can quickly make e-mail storage limits a false economy. Further, employees making individual decisions on which information to keep and to delete reduces assurance that an organization is archiving all the information required by law.

- **Business continuance and documentation benefits.** Reducing the cost of access to archived e-mail and the ability to find specific information can be critical in documenting and auditing business transactions in case of disputes. It can be particularly valuable in documenting activities of employees who may have left the organization, are on vacation, or are otherwise unavailable to report on business they conducted for the company.

Customer Success with Enterprise Vault

The following short case studies illustrate the realized business value created from using Enterprise Vault.

Webcor Builders

Organizational Overview: Webcor Builders (www.webcor.com) is the largest general contractor in the San Francisco Bay Area with assignments as varied as high-density residential projects, luxury hotels and resorts, health care facilities, and biotech facilities.

Solution-at-a-Glance for Webcor Builders

Challenges:

- Maintain competitive advantage by using e-mail as primary means of communication
- Reduce IT costs associated with searching and retrieving e-mails needed for regulatory compliance and legal subpoenas
- Support e-mail archiving needs of both stationary and mobile users

Solution:

- Veritas Enterprise Vault
- Veritas Technical Support

Benefits:

- 100% ROI for Enterprise Vault in 10 months
- 100% ROI for Discovery Accelerator after first use

Benefits continued:

- 25% reduction in total cost of ownership for enterprise e-mail
- 50% annual growth in number of mailboxes accommodated without any increase in IT staff
- 45% reduction in e-mail maintenance costs
- \$35,000 saved in IT staff time and \$20,000 saved per year in attorney staff time through more efficient discovery searches
- 40 hours of IT technician time saved per subpoena
- \$10,000 every two years saved by avoiding purchases of additional Microsoft Exchange servers and storage
- Able to comply with HIPAA, Sarbanes-Oxley, California state requirements for records retention

Challenges: E-mail—for both stationary and mobile users—is a business-critical mode of communication for Webcor, which is faced with massive amounts of communications transmitted via e-mail. Even though the firm is privately owned, many of its clients are publicly traded, so Webcor must follow Sarbanes-Oxley guidelines and must be able to deliver requested information in the event a client is audited. In addition to significant costs and time requirements associated with manual IT searches for requested e-mail, Webcor faced potential risks by having IT staff read through the trails of e-mail; IT staff could be subpoenaed to testify on behalf of or against a client.

Solution: Webcor turned to Symantec for an e-mail management solution based on Veritas Enterprise Vault software. The construction company added Discovery Accelerator for legal discovery, which includes the ability to generate detailed reports that show keywords used in the search. The legal staff now performs their own e-mail searches, using the list capability as an audit tool, which includes retention of all search queries. For installation and ongoing support, Webcor tapped Veritas Technical

“The search results from Veritas Enterprise Vault with the Discovery Accelerator Agent are terrific, much better than Microsoft Outlook’s built-in tools. We get a highly relevant set of documents based on multiple search terms we supplied, which minimize the time our attorneys spend reviewing e-mails.”

Gregg Davis
Senior Vice President and CIO
Webcor Builders

Support.

Benefits: Webcor is realizing tangible cost savings—an aggregate of \$90,000 annually—via its use of Enterprise Vault software. While maintaining Microsoft Exchange storage at 70 gigabytes and current IT staffing levels, Webcor

reduced the number of e-mail boxes by 50%. This translates into \$10,000 on additional servers and storage and \$35,000 in IT staff time. In just 10 months, Webcor recovered its investments in Enterprise Vault software and reduced its e-mail management total cost of ownership by 25%. Maintenance windows are smaller as well, which have reduced e-mail maintenance costs by 45%. Savings extend to the time spent performing manual searches, which Webcor estimates at \$35,000 annually in productivity savings.

Advantage Sales and Marketing LLC

Organization Overview: Established in 1988, Advantage Sales and Marketing LLC (www.asmnet.com) has become a leading sales and

Solution-at-a-Glance for Advantage Sales and Marketing LLC

Challenges:

- Ensure reliable e-mail service for growing number of employees
- Minimize expense and inefficiencies of dealing with spam
- Accommodate communication requirements for increasingly mobile workforce
- Minimize capital and operating expenses for e-mail infrastructure

Solution:

- Veritas Enterprise Vault
- Symantec Brightmail AntiSpam

Benefits:

- \$225,000 saved annually in e-mail administrative expenses
- 60% savings on initial e-mail infrastructure hardware and software investments
- 90% reduction projected in e-mail storage requirements
- 40% growth in archived e-mail without any headcount increases
- 120 million spam e-mail messages filtered out annually, with 99.999% accuracy

marketing agency specializing in the consumer packaged goods industry in the past five years. Today, the company represents over 1,200 clients, including GlaxoSmithKline, Unilever, Schering-Plough, Del Monte, Quaker Oats, Tropicana, and Gatorade.

“Our e-mail is more than just business critical—it’s the lifeblood of Advantage Sales and Marketing communications. That’s why we chose Enterprise Vault and Brightmail AnitSpam software from Symantec. They add the availability and security that we need to be consistent and successful for years to come. In addition, the combined solution has saved us 60% on our hardware and software acquisition costs.”

William Hiatt
National Technology Director
Advantage Sales and Marketing LLC

Challenges: With more than 30 different companies underneath one umbrella, a number still growing through corporate acquisition, Advantage Sales and Marketing sought to reduce cost and complexity by centralizing its e-mail system. Key factors that weighed in the consideration of a software infrastructure solution included controlling spam, making e-mail accessible while containing storage costs, and seamlessly integrating all users via standard interfaces and information repositories.

Solution: The initial step was to implement a solution that would help the sales and marketing agency to filter out more than 120 million annual spam. Assuming an average of five seconds to delete each spam message, Advantage Sales and Marketing was spending approximately 156,000 hours annually—or the equivalent of 83 employees—dealing with spam. The company implemented Symantec Brightmail AntiSpam software because of its ability to deliver virtually no false positives.

The next step was to address burgeoning e-mail storage volume with an archival and e-discovery solution based on Veritas Enterprise Vault from Symantec. Leveraging the compression and single instance storage functionality in Enterprise Vault, Advantage Sales and Marketing is able to store only one copy of an attachment instead of every copy made and sent. Enterprise Vault also offers Advantage Sales and Marketing the ability to provide remote users with offline accessibility, an important requirement since the sales force for Advantage Sales and Marketing is highly mobile.

Benefits: No IT support staff—saving of \$225,000 longer shackled with the time required to identify and delete spam, Advantage Sales and Marketing is saving approximately \$2.5 million annually through improved employee productivity. Enterprise Vault is saving 60% on e-mail hardware and software acquisition costs, including reducing the

amount of projected storage needed for e-mail by an estimated 90%. In addition, though experiencing 40% growth in e-mail storage volume, by leveraging Enterprise Vault, Advantage Sales and Marketing was able to avoid the addition of three additional (using an average mean salary of \$75,000 annually).

Symantec Corporation

Organization Overview: Prior to its merger with Symantec in June 2005, VERITAS Software had grown to more than US\$2 billion in annual sales and 7,500 employees worldwide. Like many companies of this scale, VERITAS managed an ongoing workload of legal actions, financial reports, and regulatory disclosures requiring searches of the company’s e-mail archives.

Challenges: By January 2005, VERITAS recognized that its incumbent archiving solution, which relied on searches through backup tapes, unconsolidated PSG servers, and other resources, cost too much to operate and could not assure complete retrieval of requested information. In addition, the company’s legal counsel generated 50 to 100 archive queries annually, with each inquiry consuming 50 to 100 person-hours for the IT department to process. Even if the lowest estimate of workload is used—50 inquiries per annum times 50 hours per inquiry—the resulting 2,500 hours of work time represents the equivalent of a full-time employee dedicated to performing legal and regulatory archival searches.

The main impetus for an Enterprise Vault-based archiving and e-Discovery solution actually came

from VERITAS' legal department (now part of the Symantec legal department). While the legal department recognized drivers around operational efficiency and cost savings, they recognized the lack of a dedicated archiving and retrieval solution exposed the company to significant litigation and regulatory risks. Further, the trend of legal precedents in the U.S. is quickly moving in the direction that all relevant electronically-archived evidence will be available to litigators and regulators. Those with "can't-find-it" responses are deemed as hiding something damaging.

"Requirements to comply with a growing list of governmental regulations dictates that public companies—which increasingly extends to private entities in many instances—develop e-discovery solutions that allow them to respond quickly and completely to unpredictable and far-reaching requests for information."

John Brigdon
Senior Vice President and Co-Counsel
Symantec Corporation

reduce it from 50 to 100 hours per request to one to two hours per request. This should save Symantec the equivalent of salary, benefits, and capital (office space, equipment) required by a full-time system administrator, an estimated US\$100,000 cost savings.

Solution: Recognizing the value of Enterprise Vault, the VERITAS legal team elected to roll out an e-Discovery solution—starting with the legal team—across the Symantec enterprise-wide environment.

Benefits: While the Enterprise Vault implementation is in its early stages, IT management and corporate counsel staff anticipate the following benefits:

- **Archive Discovery Savings.** For the time to process archive inquiries, Symantec expects to

- **Reduced Risk.** The Enterprise Vault solution also lowers the risk of sensitive data being "flushed" from the IT infrastructure or becoming invisible to inquiries on unconsolidated resources (laptops, PDAs, etc.). As this represents a risk factor with incalculable consequences in the case a "data gap" mushrooms into a major legal or regulatory issue, the immediate, direct benefit—though significant—cannot be ascertained.
- **Cost Savings.** Though still too early to calculate, Symantec expects to reduce requirements for storage resources through compression and single instance archived data and the ability to migrate data to lower cost storage platforms

Solution-at-a-Glance for Symantec Corporation

Challenges:

- Minimize expense and inefficiencies of dealing with legal inquiries
- Reduce exposure to litigation through dedicated archiving and retrieval solution

Solution:

- Veritas Enterprise Vault

Benefits:

- US\$100,000 cost savings estimated from improved archive discovery process
- US\$15.6 million savings from improved e-mail administration once enterprise vault is deployed across entire enterprise.
- Reduced risk of losing valuable and pertinent e-mails for legal inquiries

- **E-Mail Administration.** The Enterprise Vault deployment reduced staff time required to self-administer e-mail storage, estimated to consume one hour of employee time per week. At one hour per week for 52 weeks a year involving 15,000 employees, this represents an eventual productivity gain—once Enterprise Vault is rolled out across all Symantec employees—of adding the equivalent of 156 employees at minimal cost, or a gross benefit of \$15.6 million, less the cost of buying, installing, and administering the Enterprise Vault solution.

Conclusion

Legal discovery and regulatory compliance have added significant costs to conducting business for private and public sector organizations worldwide.

As organizations depend on information technology to enable business processes of all kinds, the IT department plays a crucial role in discovery impact and regulatory compliance impact-mitigation efforts. Further, e-mail and related messaging technologies have been recognized as particularly important information sources for regulators and litigation attorneys seeking evidence about an organization's operations and decision making.

Properly planned and executed IT programs to support legal discovery and regulatory compliance can make significant and measurable contributions in several areas:

- Lowering the risk of regulatory non-compliance for information retention, monitoring, and supervision while simultaneously lowering the risk of a weak legal defense from inadequate record keeping
- Reducing cost of storage to support information archiving

- Reducing cost of responding to requests for archival information
- Improved employee productivity by centralizing e-mail storage management

Enterprise Vault software, when deployed as part of a comprehensive e-mail and messaging archiving solution, is providing private and public sector organizations with the ability to design and execute a discovery and/or regulatory compliance solution for their business and organizational needs. These benefits have been experienced by multiple enterprises and can be measured and projected through quantitative return-on-investment analysis techniques.

While every organization faces widely varying business requirements and exposure to government regulation and the legal

system, Enterprise Vault software merits strong consideration by organizations seeking to reduce the costs and risks associated with discovery and compliance, while also improving employee productivity through more efficient administration of e-mail and messaging services.

“The Veritas Enterprise Vault solution from Symantec provides robust, function-rich archiving, discovery, retrieval capabilities that enable us to do exactly that. In addition to the benefits of compliance, we are realizing very tangible business value from its deployment.”

John Brigdon
Senior Vice President and Co-Counsel
Symantec Corporation

¹ Plotkin, Jeffrey, “E-Mail Discovery in Civil Litigation: Worst Case Scenarios vs. Best Practices,” April 2004.

² Osterman Research, “The Great E-mail Question: Purge or Store?,” November 2005.



E-Business Strategies, Inc.

R&D for Next-Generation Solutions

4080 McGinnis Ferry Road
Suite 603
Alpharetta, GA 30005

Phone: (00-1) 678-339-1236
Fax: (00-1) 678-339-9793

E-mail: contact@ebstrategy.com

Visit us on the Web:
www.ebstrategy.com

E-Business Strategies (ebs) is a technology research and ROI consulting practice.

Since its inception, the company's focus has been on the 3C's — Conceptualize, Communicate and Create. Known for our real-world experience, consultative style, and pragmatic approach, ebs provides strategic guidance to clients by delivering analysis, market research, white papers, and consulting services.

ebs is committed to helping its clients overcome market challenges and improve their business practices. ebs specializes in e-business, mobile solutions, business process outsourcing (BPO), offshore outsourcing, CRM, and Supply Chain processes and technology architecture.

Focused on information technology enabled solutions, the company offers cutting-edge research, customized ROI consulting services, and innovative educational programs. ebs services are designed to give companies the ability to sense, adapt, and respond quickly to changes in the marketplace.

The information contained in this report represents the current view of E-Business Strategies (ebs) on the issues discussed as of the date of publication. It should not be interpreted to be a commitment on the part of ebs or VERITAS, and ebs cannot guarantee the accuracy of any information presented after the date of publication.