Strategic Information Management Through Data Classification
Reducing Corporate Risk and Cost by Gaining Control of Business Information Assets

by
Glen Day
day_glen@bah.com

Booz | Allen | Hamilton
delivering results that endure
Strategic Information Management Through Data Classification
Reducing Corporate Risk and Cost by Gaining Control of Business Information Assets

Even in the midst of a global recession, enterprise storage demand continues to grow at a feverish pace. In addition to bearing escalating costs for storage and related services, companies are also facing increasing risk of data breaches due to the pervasiveness of how and where confidential files are stored. Despite significant investments in content management and data leak protection technologies, most businesses still lack the core processes and tools needed to effectively manage vast amounts of digital data in accordance with business objectives and compliance mandates. Providing businesses with the capabilities necessary to effectively manage and protect information assets demands a more strategic and comprehensive approach to today's information management programs.

This paper provides a better understanding of how exponential data growth directly affects the risk posture of critical corporate information assets, and addresses the common problems caused by gaps in information management programs and the likely consequences associated with immature methodologies. It also highlights the business advantages and the privacy compliance benefits that can be realized with an effective data classification program that applies a holistic approach to information management.

More Data, More Cost, More Risk
Over the past few decades, most companies made a strategic decision to provide increasing IT resources to their employees. As a result, Moore’s Law prevailed not only in processing power, but also in storage disk capacity. For the past few decades, the price of a gigabyte of storage has been dropping by 30 percent per year, on average. A company having insufficient storage is now virtually unthinkable. Despite a slowing economy, the storage industry in the United States grew by 15 percent between 2007 and 2008 (IDC, 2008).

IDC estimates that information is now growing by 60 percent per year and will continue to grow at that rate through 2011. Worldwide, digital information will escalate tenfold between 2006 and 2011, from under 200 to almost 2,000 exabytes. However, not all of this digital information is stored safely in the corporate database where it can be managed, monitored, and controlled. Enterprise Strategy Group estimates that between 80 to 85 percent of all business data is unstructured (ESG, 2007), much of this in the form of e-mails, text documents, spreadsheets, and presentations (.doc, .ppt, .xls, and .pdf).

Unstructured data is considered the most evasive and unmanaged data format within any company; this poses great risk to businesses. Few hurdles prevent employees from copying confidential data from secure databases and storing the same information in a spreadsheet, thereby negating any security measures protecting its access, use, and dissemination. This kind of violation is often perpetrated by employees to provide
convenient access to information while in transit or traveling. Unfortunately, this practice can lead to serious security and privacy breaches, as laptops and USB storage devices with insufficient security controls to protect sensitive data are often lost or stolen.

With corporate data increasing exponentially, what are the ramifications of having the storage environment grow 30 percent faster than a company’s revenue or IT budget? With a 30 percent annual average price decline, a simplistic view suggests just purchasing more disks. However, this tactic promises more than it delivers. Related incremental costs for staff and storage management services such as backup, antivirus, and data replication continue to escalate unabated.

Over time, most business information devolves from being an information asset to being an information liability—it no longer serves a business need yet still requires care, protection, and incurs costs. The challenge is not to restrict the growth of useful business data considered to be valued assets, but how to better manage and dispose of expired or worthless data. This useless information is expensive to maintain, holds no further business value, and continues to present a high business risk.

The increasing threat of data leakage remains a primary business challenge. A recent Wall Street Journal article reported that the number of data breaches increased by almost 50 percent in 2008, compared to the previous year, exposing the personal records of some 36 million people to potential thieves (WSJ, 2009). The Ponemon Institute found that these breaches cost companies nearly $200 per record stolen, or $6.6M per incident. The more data stored by an organization, the higher the risk of a breach. Given the exponential increase in data breach incidents, if a casualty has not yet occurred, odds are that one is imminent (ponemon.org).

Until recently, TJX Companies, parent company of retail giant T.J. Maxx, held the record for the largest single security breach of sensitive customer information. On January 21, 2009, Heartland Payment Systems, a large credit card payment processing company, eclipsed TJX when Heartland announced the discovery of malicious software installed on the company’s systems. As Heartland processes more than 100 million transactions per month, the number of compromised records could be in the hundreds of millions. At $200 per record stolen, the financial hit to Heartland could be devastating (Claburn, 2009).

In 1999, congressional lawmakers Phil Gramm, Jim Leach, and Tom Bliley pushed through the Gramm-Leach-Bliley Act, the first major piece of legislation that specifies measures companies must take to protect Nonpublic Personal Information (NPI). This became the foundation for many other privacy regulations—such as HIPAA and the Payment Card Industry (PCI) initiative, mandating protection of sensitive patient and customer data, respectively. In a post-9/11 world, other new regulations like the International Traffic in Arms Regulations (ITAR) place additional restrictions on the flow of trade information. New attention is now focused on the shipment of microchips and electronics, as well as related electronic information surrounding these devices. This spotlight places further duties and burdens on businesses. To properly distribute information internationally related to the manufacture of these components, one may have to effectively classify and restrict access to thousands or even millions of files and stored e-mails.

A Growing Data Management Challenge

Until recently, these problems were relatively manageable. In cases where unstructured data needed to be closely managed for a regulation such as HIPAA or ITAR, companies could employ Enterprise Content Management systems. For a small pool of data, such as the CEO’s e-mail or a repository of engineering documents relevant to litigation, businesses could use litigation support software or services. If data in specific folders or behind certain applications needed to be protected, they could use Identity Management and Data Loss Prevention solutions.

Those solutions assumed some logical concentration of relevant data, either in a few places or as a manageable size. Unfortunately, these assumptions are no longer valid. Data held by Fortune 500
companies can no longer be measured in single terabytes and typically exists in multi-petabyte heterogeneous storage environments spread out across global networks. There are multiple silos of information, in many cases governed by data stewards with authority to create their own policies based on regional or departmental priority.

Most companies do not have adequate processes or technologies to manage their unstructured data. 75% said they were concerned that their unstructured data was growing too rapidly. 63% said they did not have adequate systems to manage it.

- Computerworld survey of 250 large companies on data management

On average, most large corporations now have over 240 terabytes of storage, of which some 80 terabytes may be subject to significant requirements for information protection, such as access and lifecycle controls. Relevant and supporting enterprise policies or solutions for meeting those requirements are often immature and insufficient. The digital data, and its management requirements, have simply grown too fast for most companies to build an effective information management strategy that can meet business objectives.

Continuing to neglect these challenges may result in: adverse legal judgments for failing to meet Federal Rules of Civil Procedure (FRCP) guidelines; penalties; and lost business resulting from data privacy breaches, or loss of trade secrets that could diminish a company's competitive edge. Effectively employing an information management strategy may be the single largest priority for Fortune 500 companies over the next 3 years.

Answering the Challenge
Gaining control of corporate information assets will not be accomplished through technology solutions or ad hoc process changes. In Booz Allen’s view, enterprises should implement a strategic information management program by first classifying data to help reduce their corporate risk exposure, decrease information discovery times, improve compliance status, and potentially realize significant cost savings through an effective data disposal program.

There are substantial synergies between information management and other enterprise-wide shared services, including access management, data leakage protection, records management, litigation support, storage management, governance, risk, and compliance. Our comprehensive approach takes a holistic view of key business processes and data protection controls as assessed against our information management adoption model in Exhibit 1.

New rules and regulations governing how data must be stored, secured, transferred, retained, disposed of, and used will encourage many businesses to emulate the standard set by US military and intelligence communities in establishing a classification schema.

Exhibit 1 | The Booz Allen Strategic Information Management Model (SIMM)

Source: Booz Allen Hamilton
For almost a century, Booz Allen Hamilton has assisted federal agencies and commercial companies in building strategies to streamline their operations and gain a competitive advantage. More recently, Booz Allen has helped to pioneer strategies for large organizations to solve enterprise problems related to records management and information security. This unique experience and expertise has never been more relevant for commercial companies with global operations.

**Effective Information Management Through Strategic Data Classification**

The majority of data and privacy breaches are avoidable. Traditionally, organizations have applied a network-centric focus to securing systems, based on defined confidentiality levels for storing and processing data. While still a necessary component, a more information-centric approach is needed today. Better control and protection of confidential and sensitive information first requires an awareness of where the data is stored and how it is protected.

Booz Allen’s methodology conveys the complexities of information management in simple business terms:

- Know what information you have
- Know where you have it
- Know what information you have to keep
- Know why you have to keep it
- Keep it only as long as you need to—dispose of everything else

Booz Allen’s strategic approach to building and executing a data classification program, as illustrated in Exhibit 2, is derived from a logical and comprehensive workflow.

- **Classification Schema Definition:** Prior to classifying unstructured data, business owners must first determine the levels of classification (Confidential, Restricted, Public, etc.) and what attributes constitute each of the levels (SSN, credit card number, financial information, protected health information, etc.).

- **Discovery:** Once classifications are defined, storage managers should identify known storage areas and query for unknown storage devices.

- **Data Mapping:** Detailed data maps should then be created to formally document leading data flows and their associated classifications.

- **Analysis:** During this critical phase, stakeholders should perform a detailed review and evaluation to identify violations and conflicts between corporate policies and user practices as related to information handling.

- **Strategic Realignment Plan:** Based on the outcomes from the previous phases, remediation recommendations should be developed using risk-based methodologies to create a strategic plan to realign both administrative policies and user practices. This should include an information security control enhancement plan to mitigate the identified deficiencies.
Applying Booz Allen’s business-centric approach to data protection through strategic data classification is an essential element in corporate risk reduction efforts. This approach will reduce risk, improve compliance, speed information discovery, and—through data disposal of expired files—decrease costs.

**Conclusion**

Storage capacities are growing exponentially, exacerbating the number and severity of data breaches and other security issues. Whether due to hackers or employees, companies are at risk of losing or compromising information assets on a daily basis. In this difficult economic environment, companies need to consider a comprehensive, strategic approach to information management through data classification. With decades of relevant experience, Booz Allen Hamilton is the most qualified partner to help drive the adoption of government best practices and proven methodologies for information security and management in the commercial sector.

Booz Allen has helped customers at various stages of the planning and buying cycle. While some clients continue to struggle to assemble internal project teams, others have matured their programs to include high automation. Booz Allen offers services at all levels of the adoption cycle and specializes in translating business requirements to policy definitions and recommendations for enterprise solutions.

Discerning business leaders rely on Booz Allen to deliver quality results to help resolve their complex business challenges. Leveraging our team of experienced cybersecurity experts, proven methodologies, and a reputation built on decades of success, Booz Allen works as your trusted advisor to help protect your business with enduring results.
About the Author

Glen Day is a Principal in Booz Allen Hamilton’s Los Angeles office who leads the firm’s cyber security and privacy services for commercial healthcare. Glen works with our clients to mature and optimize their security and privacy programs to effectively protect their IT assets and meet compliance mandates. Previously, as Los Angeles County’s first Chief Privacy Officer, he was responsible for the development and implementation of HIPAA’s privacy policies and practices, working across several departments and hospitals to drive the county’s health privacy excellence.

Glen also has held executive positions for IT operations and cyber security at various start-ups, and is a retired Commander from the US Navy. He earned his MS in Information Management from the Naval Postgraduate School and his BS in Applied Mathematics from the University of Southern California.

Contact Information:

Glen Day
Principal, CISSP, CISM
Cyber Security & Privacy
day_glen@bah.com
310/297-2120

Sources

Claburn, Thomas, “Heartland Payment Systems Hit by Data Security Breach,” InformationWeek, January 20, 2009
Enterprise Strategy Group, Extending Discovery to All Corporate Information, December 2007
IDC, The Diverse and Exploding Digital Universe, March 2008
About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for 95 years. Every day, government agencies, institutions, corporations, and infrastructure organizations rely on the firm’s expertise, and objectivity, and on the combined capabilities and dedication of our exceptional people to find solutions and seize opportunities. We combine a consultant’s unique problem-solving orientation with deep technical knowledge and strong execution to help clients achieve success in their most critical missions. Providing a broad range of services in strategy, operations, organization and change, information technology, systems engineering, and program management, Booz Allen is committed to delivering results that endure.

With 20,000 people and $4 billion in annual revenue, Booz Allen is continually recognized for its quality work and corporate culture. In 2009, for the fifth consecutive year, Fortune magazine named Booz Allen one of “The 100 Best Companies to Work For,” and Working Mother magazine has ranked the firm among its “100 Best Companies for Working Mothers” annually since 1999.

To learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit www.boozallen.com.
## Principal Offices

<table>
<thead>
<tr>
<th>ALABAMA</th>
<th>KANSAS</th>
<th>OHIO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Huntsville</td>
<td>Leavenworth</td>
<td>Dayton</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CALIFORNIA</td>
<td>MARYLAND</td>
<td>PENNSYLVANIA</td>
</tr>
<tr>
<td>Los Angeles</td>
<td>Aberdeen</td>
<td>Philadelphia</td>
</tr>
<tr>
<td>San Diego</td>
<td>Annapolis Junction</td>
<td></td>
</tr>
<tr>
<td>San Francisco</td>
<td>Lexington Park</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Linthicum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rockville</td>
<td></td>
</tr>
<tr>
<td>COLORADO</td>
<td>MASSACHUSETTS</td>
<td>SOUTH CAROLINA</td>
</tr>
<tr>
<td>Colorado Springs</td>
<td>Boston</td>
<td>Charleston</td>
</tr>
<tr>
<td>Denver</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MICHIGAN</td>
<td>TEXAS</td>
</tr>
<tr>
<td></td>
<td>Troy</td>
<td>Houston</td>
</tr>
<tr>
<td></td>
<td></td>
<td>San Antonio</td>
</tr>
<tr>
<td>FLORIDA</td>
<td>NEBRASKA</td>
<td>VIRGINIA</td>
</tr>
<tr>
<td>Pensacola</td>
<td>Omaha</td>
<td>Arlington</td>
</tr>
<tr>
<td>Sarasota</td>
<td></td>
<td>Chantilly</td>
</tr>
<tr>
<td>Tampa</td>
<td></td>
<td>Falls Church</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Herndon</td>
</tr>
<tr>
<td>GEORGIA</td>
<td>NEW JERSEY</td>
<td>McLean</td>
</tr>
<tr>
<td>Atlanta</td>
<td>Eatontown</td>
<td>Norfolk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stafford</td>
</tr>
<tr>
<td>HAWAII</td>
<td>NEW YORK</td>
<td>WASHINGTON, DC</td>
</tr>
<tr>
<td>Honolulu</td>
<td>Rome</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The most complete, recent list of office addresses and telephone numbers can be found on www.boozallen.com by clicking the “Offices” link under “About Booz Allen.”