Crowe Horwath

Crowe Horwath Global Risk Consulting Limited
Independent Member Crowe Horwath International

Big Data: Strategic Risks and Opportunities

Looking Beyond the Technology Issues

A White Paper by Richard Anderson and Daniel Roberts
September 2012

Today's organizations retain more data than ever before and are rapidly developing ways to access and analyze this data for strategic, operational, and competitive advantage. Risk management professionals have an important role to play in helping their organizations to exploit big data capabilities at minimal risk – while also using these same big data approaches to improve the way they perform their own duties.

Over the past decade, the volume of information that is collected, processed, and retained by organizations has multiplied dramatically. Today most companies retain vastly more data about their customers, suppliers, and competitors – not to mention their own operations, employees, and overall business environment – than they ever have before.

Exploiting these vast reservoirs of information is the general purpose of the concept known as "big data," which can be loosely defined as the tools, processes, and procedures that allow an organization to create, manipulate, and manage very large data sets and storage facilities – volumes of data that are beyond the capabilities of most commonly used software tools.[1] While many companies are making significant strides in this area, for the most part businesses hold the information in their systems without using it to its full advantage.

An important point that is often overlooked when trying to capitalize on big data's potential is that these large, unexploited opportunities also can pose large, unrecognized risks. The steps being taken to exploit these data pools can backfire in unexpected ways, which is why risk management professionals must play an active role in the effort.

For example, in a recent story on the use of sophisticated data analysis tools in screening potential employees, The Wall Street Journal pointed out, "Data-based hiring can expose companies to legal risk. Practices that even unintentionally filter out older or minority applicants can be illegal under federal equal opportunity laws."[2]

Recruiting and hiring practices represent just one of the many areas in which big data is now being applied, yet the risks in this area are illustrative. Based on comments from one of the employment lawyers interviewed, the Journal article noted, "Bigger data sets can raise the risks of violating the law by increasing the number of statistical relationships that could unwittingly screen out protected groups…. But they also could make it easier for companies to prove that the factors being measured are relevant to the job being filled."

This same principle applies in the many other functions in which big data is employed. The greater the amount of data, the greater the risk. But conversely, the greater the amount of data, the greater the opportunity to mitigate risk as well.

Any time an organization uses big data to make decisions, there is risk that it could be misused or used ineffectively. Auditors and other risk professionals obviously should monitor big data use to address this risk. At the same time, though, auditors and risk managers also can use big data to improve their own operations. Beyond alerting the organization to new areas of potential risk, risk managers also should be approaching big data in a proactive manner, identifying opportunities to use large data sets in new ways that will enable the internal audit and risk management functions to operate with greater efficiency.

In both of these functions – reacting to new risks specifically related to big data and exploiting big data to identify and mitigate existing risks – auditors, risk managers, and compliance officers have important roles to play.

Trends – The State of Data Today

Large organizations today need to maintain large amounts of both structured and unstructured data for operational and compliance purposes. The volume of stored data has increased exponentially, reflecting the effects of Moore's law, which predicts, in general terms, that the storage capacity of integrated circuits doubles roughly every two years.[3]

Since Gordon Moore's original observation along these lines in 1965, one obvious consequence has been a dramatic reduction in the cost of computing, enabling organizations to manage more processing power, storage, and data transfer speeds for substantially less cost. For example, back in the 1980s IBM reportedly recommended that its clients plan to employ one data management professional for every five gigabytes of data stored on their IBM mainframes (less than can now be stored on a small flash drive). Today, by way of contrast, one author estimates that 2.5 quintillion bytes of data (a quintillion is 1 followed by 18 zeros) are created every day.[4] Twitter alone now handles 400 million messages a day.[5]

Concurrent with this almost unfathomable growth in computing power and storage capacity has been a comparable growth in the number of ways unscrupulous operators can exploit security lapses and other vulnerabilities in organizations' data systems to gain access to personal information or other sensitive data. Headlines announcing severe data breaches and the theft of sensitive information have become all too common.

The regulatory climate has evolved in response to these events, which in turn increases the compliance risk associated with big data. For example, the most recent European Union Data Protection Regulation, released in January 2012, extends the scope of the EU data protection law to all foreign companies that process personal data of European Union residents.[6] In an increasingly globalized economy, the rules are becoming ever more complex for financial institutions – and, for that matter, all organizations with customers or operations in more than one country – that must now comply with multiple regulations about how they store, access, and share personal information.

These changing regulatory requirements are occurring at the same time that such accumulated data is increasingly recognized as a valuable asset in its own right. The use of big data to improve organizations' marketing and customer outreach efforts is growing consistently, enabling them to target their product service offerings more precisely to individual customers' perceived interests.

The task facing auditors and other risk management professionals in this environment is twofold: First, they must help their organizations identify the previously unforeseen risks that the use of big data can pose. At the same time, they must be alert to the opportunities big data offers the risk management function itself.

All too often, however, much of risk management is still being done in a "data-light zone." Large organizations' data warehouses store a wealth of information – from emails, ledgers, and customer relationship management (CRM) system data to images, video, tweets, and blogs – that could be extremely beneficial in their risk management processes. Unfortunately, there are often significant gaps between what is possible in this area and what is achieved.

Gaps – Assessing What's Still Unknown

As organizations grapple with big data trends, they must work to close the gaps between "what is" and "what could be." These gaps can be grouped into several basic categories:

- **Technological gaps.** As already noted, the volume of information that is being stored as part of the ordinary course of conducting business is growing exponentially. Organizations' ability to tap into all this data and release the value has not kept pace with the size of the opportunity. Technology teams often struggle to support large data systems that threaten to overwhelm their existing technical infrastructures. Such technical concerns can distract organizations from focusing on how to use the data in a constructive manner.
- **Legal and policy gaps.** While some jurisdictions limit the use of personal data, in other instances the collection and analysis of data are largely unrestricted. In addition, certain regulatory requirements, such as anti-money-laundering regulations, require businesses to develop an unprecedented level of insight into customer behavior and activities. Conflicting or inconsistent privacy frameworks make it more challenging to manage large volumes of data efficiently, in a way that allows access when needed but limits access when prohibited.
- **Failure to recognize data-driven risk.** As marketing, customer service, and strategy development teams become more adept at making good use of the massive amounts of data they can access, it is easy to become dazzled by the potential benefits while failing to foresee the possible negative consequences. This unforeseen downside is not confined to security breaches. For example, businesses that use sophisticated analytics to perform highly targeted marketing campaigns can quickly alienate customers who sense that the business knows more about them than the customers are comfortable revealing – or that they would want revealed to others.

- **Failure to capitalize on big data risk mitigation capabilities.** The large volumes of data now held on enterprise systems are often not well mined or well analyzed for risk management purposes. For example, data mining can enable a much more efficient audit process by allowing auditors to focus more quickly on critical areas rather than expending time and resources in manual testing. At the policy level, this failure often can be recognized by the absence of key risk indicators (KRIs) for each business or group, or by the lack of a uniform, organizationwide set of KRIs.

Challenges – A Broader View of What's Missing

In working to address their data-related gaps and vulnerabilities, organizations of all types can expect to encounter certain recurring challenges. These represent the high-level milestones that must be accomplished in order to mitigate the risk and capitalize on the potential associated with the big data concept. Both risk management professionals and the senior executive and managerial levels of the organization – each in their own way – must see to it that these essential steps are achieved:

- **Develop oversight and guidance at the board level.** On the one hand, the additional and powerful insights that big data can deliver are very appealing. On the other, there are potentially significant legal, compliance, ethical, and commercial risks associated with unfettered exploitation of the data. If boards and audit committees lack a clear understanding of the need, role, and potential of big data, they often are unsure how to lead the effort or respond to the potential challenges. It is the responsibility of senior managers and executives – drawing on the specific expertise of risk managers and auditors – to make sure the board adequately understands these issues so that it can perform its governance function effectively.
- **Identify needs before seeking solutions.** There is a natural tendency to define an organization's needs in terms that reflect already known solutions and approaches. This is particularly likely when working with technology providers to develop new software applications for managing and analyzing large quantities of data. Rather than defining the problem to fit the available solutions, organizations must first take a step back and think what they might be able to do, identifying strategic and visionary opportunities, before engaging in the search for vendors' software.
- **Coordinate real-time and historical data.** Historically, many businesses have had little need for real-time monitoring capabilities. For example, most organizations have large volumes of information in their accounting systems to tell them what happened in the past. The challenge is how to accurately draw from this information to develop real-time KRIs that are predictive. Often, large amounts of data are outdated and require filtering before they can be used for strategic purposes. A simple extrapolation from the past can be very dangerous.
- **Address organization-specific issues.** In addition to meeting the commonly recurring challenges just mentioned, each organization will face its own specific hurdles regarding coordination and communication across divisions or lines of business. These can include language barriers, technological limitations, and differences in localized goals and priorities. In such situations,

it can be quite challenging to develop consistent, companywide KRIs. In addition, at the technical level, decentralized enterprise resource planning (ERP) systems and siloed data often make it difficult to establish centralized data warehouses and to organize disparate data into a usable format.

Solutions – Developing a Plan for Action

From a risk management perspective, any effort to improve the management of today's large reservoirs of data must approach the challenge on both fronts: 1) it must mitigate the strategic risks associated with using big data initiatives to boost performance, improve sales, and achieve other strategic goals; and 2) it must develop ways to use big data to perform the risk, audit, and compliance functions more efficiently. In other words, the objective is to both "increase the gain" and "reduce the pain."

Each organization will develop its own particular approach for doing this. In general, however, a successful approach will occur over the course of five broad phases. Note, that these five phases often overlap and do not necessarily occur in a step-by-step sequence. In addition, both risk management professionals and the organization's senior management have specific tasks they must accomplish in each phase in order to make the process work.

Phase 1: Identify Roles and Responsibilities

The roles of risk, audit, and compliance professionals in supporting and developing big data approaches should be clearly defined at the outset. As new strategic, marketing, customer-service, and operational initiatives are launched and championed by other groups, it is essential that risk and compliance professionals be engaged in the process of determining if there are issues that require C-suite or board-level attention. Just as a manufacturer would not launch a new product without extensive testing, any new information-driven initiative should be thoroughly tested to identify potential strategic and regulatory compliance risk.

Concurrent with this role, risk and compliance professionals should engage education and awareness building in order to develop a proper focus on risk among marketing, research and development, and other functions that use big data. At the same time, they should tap into the capabilities of these groups to help them to exploit available data to improve the efficiency of the audit and compliance processes.

Finally, the organization's senior executive and management team must exercise leadership so that risk management professionals are prepared to address both sides of the risk-related uses of big data. At the same time, they are responsible for making sure the board understands these issues, so that the next phase can be performed effectively.

Phase 2: Define Goals and Priorities

Another critical early step is clearly defining and prioritizing the goals the organization hopes to achieve by using big data. As with any high-level function, this definition must be directed at the executive level with general board oversight, but its success ultimately will depend on those who are actually involved in developing the big data approach for input and expertise. These contributors include the potential users of big data – strategists, marketers, researchers, and operational managers – as well as the IT team and the risk and compliance professionals.

Phase 3: Assess Critical Data Issues

With goals and priorities established, a closely related activity is assessing the critical data-related issues that are likely to arise as these initiatives are undertaken. These issues may include matters such as privacy concerns, the degree of transparency required for regulatory compliance, existing data silos, necessary firewalls that either exist or must be constructed, and existing firewalls that should be removed. Both the risk management and executive teams should be actively involved in this effort – the risk management professionals providing hands-on expertise and counsel and the executive teams making sure the issues are being addressed in ways that comply with the organization's long-term strategies and governing principles.

Phase 4: Identify Key Risk Indicators

As big data initiatives are developed, the critical data issues that were identified upfront will help to inform the risk management team as it identifies key risk indicators to be monitored. The goals are to spot troublesome trends as they start to emerge in the data and to get ahead of the curve before performance problems arise.

In this effort, risk management professionals should be particularly alert to the need to play both reactive and proactive roles in managing big data risk. In addition to monitoring and mitigating risks associated with the use of big data in various business functions such as marketing, hiring, and product development, they should be alert to opportunities to employ big data proactively as risk managers. For example, internal auditors and risk managers in financial institutions can effectively use big data techniques to identify fraud, money laundering, or other prohibited activities by identifying connections among various third parties that might not otherwise be apparent.

Phase 5: Identify Opportunities to Add Value

In businesses that are inherently data-intensive, it is possible to generate added value in the risk management element by finding new ways to derive meaningful analysis from large quantities of data. For example, one insurance brokerage recently uncovered a large-scale, yet still developing, insurance fraud scheme by employing big data techniques to discover that various individuals – with completely different names and no apparent relationship – were all connected to known fraudsters by way of interconnected telephone numbers, addresses, and company names. This ability to capture several sets of data, cross-check across various data types, and then match both internal and external data would not have been available to the brokerage just a few years ago.

Even businesses that are less inherently data-driven than insurance and financial services can find comparable opportunities to add value by capitalizing on big data capabilities to improve strategy development or drive greater operational efficiency. By implementing techniques such as shared-services models – or by simply consolidating data such as that held by the accounts payable, purchasing, and payroll functions – organizations often can achieve significant administrative and operational cost savings.

The ability to achieve such value-added big data benefits requires not only proactive risk management professionals but also an attuned and aware senior management team to guide and energize the effort.

Conclusion

Businesses today are using big data not only to boost performance but also to reduce risk and prevent loss. Marketing, sales, engineering, product development, operations, logistics, and strategy development groups use big data to do smarter things faster.

As they do, their counterparts – auditors, risk managers, and compliance officers – must understand and embrace big data approaches to help identify and mitigate the risk associated with these activities. In addition, risk management professionals must take advantage of the additional opportunities big data offers for improving their own efficiency and effectiveness.

The opportunities and risks that big data presents are both significant and complex – too significant and complex to be considered solely or even primarily a technology concern. Risk and compliance managers and their teams are well positioned to help their organizations analyze and understand big data's potential, not only from a compliance perspective but also in terms of the strategic and operational advantages big data can deliver.

Contact Information

Richard Anderson is managing director of Crowe Horwath Global Risk Consulting in London. He can be reached at +44 (0) 20 3178 6833 or richard.anderson@crowehorwathgrc.net.

Daniel Roberts is director of risk services for Crowe Horwath Global Risk Consulting in London. He can be reached at +44 (0) 20 3178 6835 or daniel.roberts@crowehorwathgrc.net.

---

[1] Dan Kusnetzky, "What Is 'Big Data'?" ZDNet online blog entry, Feb. 16, 2010, http://www.zdnet.com/blog/virtualization/what-is-big-data/1708

[2] Joseph Walker, "Meet the New Boss: Big Data," "The Wall Street Journal," Sept. 20, 2012, http://finance.yahoo.com/news/meet-boss-big-data-000000184.html

[3] "Moore's Law and Intel Innovation," Intel Corp. website, http://www.intel.com/content/www/us/en/history/museum-gordon-moore-law.html?wapkw=moore

[4] Marcia Conner, "Data on Big Data," online blog entry, July 18, 2012, http://marciaconner.com/blog/data-on-big-data/

[5] Shea Bennett, "Twitter Now Seeing 400 Million Tweets per Day, Increased Mobile Ad Revenue, Says CEO," mediabistro.com online news story, June 7, 2012, http://www.mediabistro.com/alltwitter/twitter-400-million-tweets_b23744

[6] Thor Olavsrud, "EU Data Protection Regulation and Cookie Law – Are You Ready?" ComputerworldUK online news story, May 24, 2012, http://www.computerworlduk.com/in-depth/security/3359574/eu-data-protection-regulation-and-cookie-law-are-you-ready/