

Japanese M&A: poised for growth

Corporates return to pre-crisis M&A strategies
as outbound deals jump 40 percent.

Uptick in private equity secondary buyouts

Secondary buyouts can generate successful
returns for those backing them.

US entertainment & media sector – moving with the times

Companies scale back operations and
unlock value by offloading assets.

WORLDWATCH

Global mergers & acquisitions

ROUNDTABLE

Transfer pricing

BY MUAZZIN MEHRBAN



In today's digital-driven market, companies around the world are confronted with a variety of risks concerning the handling, storage and retrieval of electronic data. As a result, information security should be a key issue for most, if not all enterprises. But the challenge is to develop and maintain a data protection program that can alleviate the unique issues present in all industries. Location, operations and data flow considerations all play a part in this development. Compromised data can leave a company vulnerable to regulatory risks, such as privacy violations and reporting irregularities. Furthermore, larger corporations must assess the matter of cross-border data controls, given the growing number of outsourcing providers and sub-contractors they now utilise. Businesses should also remember that the issue of data handling is not just to protect a company from breaches but also to store its information in an accessible manner, keeping it on hand for when informed decisions need to be made. In addition, the current litigation-driven culture means that a company may be susceptible to legal and regulatory action if it fails to adequately manage its data assets.

Experts suggest that the most significant area of IT risk is data privacy and security breaches. Many companies produce large quantities of information frequently, yet fail to protect it with sufficient controls. In an effort to avoid such scenarios, regulatory bodies, including the Federal Trade Commission (FTC) and the Securities and Exchange Commission (SEC) in the US, have the power to issue substantial fines to businesses that fail to adequately protect data or mislead consumers on the level of confidentiality offered. "These regulatory bodies can also impose requirements for a business

to obtain regular outside audits of information technology risk controls for periods of up to 20 years," says Joseph V. DeMarco, a partner at DeVore & DeMarco LLP. "But the costs associated with hiring independent experts to prepare technical audits and lawyers to navigate the legal process can be significant, especially if a business is subjected to a protracted investigation or must report to a regulatory body for an extended time." Even without a regulatory response, significant failure to secure networks and databases can result in a lawsuit costing the defendant millions. This emphasises the need to adopt legal practice and technical IT controls.

In the US, the escalating trend of notification requirements for compromised data began in California. Now over 45 states across the US have adopted similar procedures and notification obligations have been embedded in sectoral laws at a federal level. Outside North America, Germany has also adopted similar measures, while supervisory bodies in the UK are placing more emphasis on enforcement cases. However, a data breach can come in any shape or size. Major US cases include that of Heartland Payment Systems, believed to have experienced one of the largest breaches in US history. "The breach related to malicious software that compromised credit and debit card data transferred through the Heartland card payment network," recalls Brian Hengesbaugh, a partner at Baker & McKenzie. "Specifically, it appears that more than 130 million credit and debit card numbers may have been affected over an 18-month period. When Heartland announced the breach, on 20 January 2009, its stock price fell 40 percent. Thirty-one separate lawsuits were subsequently filed against Heartland on behalf of consumers, investors, banks and credit unions." Heartland's

subsequent November SEC filing indicated that the total expenses, accruals, and reserves for the preceding period were in excess of \$100m. As a result, the company implemented various remediation measures to prevent future occurrences.

IT risk enforcement

In order to have an effective system in place, companies must ensure that their data security and privacy policies are implemented from the top down. Failure to prioritise data at a senior level paves the way for holes lower down. Comprehensive policies and training programs that force all areas of a company to undertake a holistic approach to managing information technology risk are therefore necessary. Such policies must conform to legal best practices and guidelines, formed through the synthesis of state, federal and local laws which all work in tandem with technical controls to lower systemic risk. In the event that a breach occurs, best practice should minimise the costs of responding to the problem. "Organisations need to exploit every available best practice for securing information, whether that is encryption, minimising intrusions, or an effective accessibility management policy," emphasises David Longson, in Global Technology Services, Storage and Data Services at IBM UK. "They need to be able to recover quickly and effectively from any natural or man-made disaster, and constantly assess the threat and risk to their key business data. By simplifying and automating a data infrastructure as far as possible, businesses can minimise the risk of significant data and financial loss." This is particularly important as the amount of data stored by a company continues to increase.

The production of documents and electronically stored data can be a monumental task if a company fails to adequately devise and implement efficient storage and retention policies.

"Before being subjected to such demands, a company should know what data it stores and where that data resides. A company should also control the amount of information it will need to search by limiting the amount of data it collects, and should retain records only as long as required by business-need or law," advises Mr DeMarco. "Of course, there are no clear dividing lines between how information is used for business operation and competitive purposes, the privacy and security of that information, and information preservation and retention."

But all three are related and companies at the forefront of information management are integrating their approach through unified policies ▶

and practices. Tackling data risk management must become more sophisticated given that attacks and risks themselves are constantly evolving, due to human nature and the fundamental role that outsourcing to third parties now plays. "Particularly within the public sector environment, there are moves to integrate huge sources of data together and distribute them more widely among the various government departments," explains Mr Longson. "This requires far more complex data storage and retrievable solutions, and the securing and backing up of data against loss becomes a significant job." In such an environment, companies must invest more and devote additional resources to this issue.

Risk management conflict

Any decision that would see new regulation attached to the control of information technology has been dismissed by experts. Many believe that businesses already have enough regulatory requirements to comply with – the proliferation of breach notification laws already serves as a significant driver to protect sensitive data. A US study by the Ponemon Institute, which conducts independent research on privacy, data protection and information security policy, showed that the average cost of a data breach during 2009 was \$204 per record, or collectively, \$6.75m per incident. This, according to experts, has proved to be a timely incentive for

businesses to take heed and protect their interests – particularly in the US financial services sector. Indeed, financial entities must deal with the constantly widening statutory and regulatory provisions under both the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act. In some industries, such as healthcare, providers and their business associates must also comply with data privacy rules under the Health Insurance Portability and Accountability Act, which were recently updated under the recent HITECH Act. In addition, there remain a host of other laws at the US state and federal levels, including certain requirements imposed under the new Massachusetts Standards for the Protection of Personal Information. Laws with regards to information risk, not just in the US but in other highly developed economies, are proliferating and rely heavily on information technology systems. But overregulation can create an environment that is actually harmful to businesses.

The US is also home to significant issues with e-discovery and litigation holds, and how these matters work with record retention policies and practices. Overseas, US businesses have to deal with the fact that non-US data privacy laws conflict with their own much fuller, robust responses to the issue. "For instance, in cases where a US company is obligated to produce evidence from global sources in a US court, the

disclosure of such data and documents could be restricted by non-US laws should non-US persons or entities be in question," Mr Hengesbaugh notes. "Laws related to data protection, privacy, bank secrecy and confidentiality all come into play, as do wider considerations such as countries unwilling to share state secrets or permit assistance with non-local government investigations," he emphasises. In one recent case, the International Revenue Service (IRS) issued a summons to financial group UBS, compelling it to disclose information related to thousands of clients with Swiss bank accounts. However, UBS explained to the court that disclosure of such knowledge would violate Swiss bank secrecy and anti-investigatory laws. Had UBS complied, it would have exposed its employees to a host of issues including fines, penalties, sanctions and even prison terms.

Globally, governments continue to introduce new laws and to focus greater attention on information technology risk. Failure to conform to these laws or follow regulatory guidelines will carry greater repercussions and graver consequences. As companies increase data storage and electronic processing, events in which data is lost will compromise a greater number of customers, which in turn will see an increase in litigation against companies, many of whom can ill-afford the additional cost given the current economic climate. ■

DISPUTES

Commercial disputes

BY SELINA HARRISON

Since the beginning of the economic downturn, all businesses have found themselves operating in an environment prone to commercial disputes. Companies are breaking agreements, challenging existing contracts, attempting to recoup losses, and fighting to preserve value where possible. As a result, corporate executives are reviewing their exposure to potential litigation. With company budgets still stretched, executives cannot afford to be unprepared. They need a clear response strategy to prevent or manage conflict. In the event of a pending legal battle, more companies are also looking to alternative dispute resolution (ADR) to avoid lengthy litigation proceedings which are costly and can damage reputations. ADR also tends to improve certainty of outcome compared to court litigation.

Disputes arising from the downturn

Commercial disputes historically escalate when financial conditions are difficult, and the global recession has been no exception. Companies struggling with cash flow problems,

burdensome operating costs, looming insolvency or threats to their competitiveness are more likely to take drastic action in an attempt to resolve the issue. If a legal avenue is available, companies may take it, even if this means open conflict with another company that leads to litigation. "In boom times, parties are more likely to resolve difficult disagreements with a compromise that gives value to both sides. But in an economic downturn, such compromise becomes more difficult and a party may have little choice but to pursue litigation to protect its interests," says David Daniels, a partner at Richards, Kibbe & Orbe LLP.

There has been an increase in complex commercial disputes in the wake of the bursting of the US real estate bubble and subsequent global financial crisis. Almost overnight, lending practices switched from generous terms and attractive pricing to stringent criteria and reduced availability. This drop in liquidity, combined with widespread reductions in revenue, squeezed companies and forced them to respond with survival measures. Restructur-

ings and downsizing became common. But such turmoil often sparks some form of conflict with employees, shareholders, creditors, suppliers, customers, regulators, or any other interested parties.

Certain sectors are more vulnerable to conflict than others. One of the most obvious, given the nature of the economic downturn, has been the financial sector. "The substantial increase in foreclosure filings has been driven by the subprime lending meltdown and other dubious lending practices that became widespread," says Michael L. Rich, a principal at Porzio, Bromberg & Newman, P.C. "Similarly, an increase in investor claims is resulting from problems in the financial sector. In the US, more scrutiny is being directed at this sector as the fallout continues from anger over TARP monies and other bailouts and declines experienced in portfolios. That scrutiny has been intensified by the current political administration in the US seeking broad reforms of certain practices in the financial sector."

But not all countries have been affected in ►►