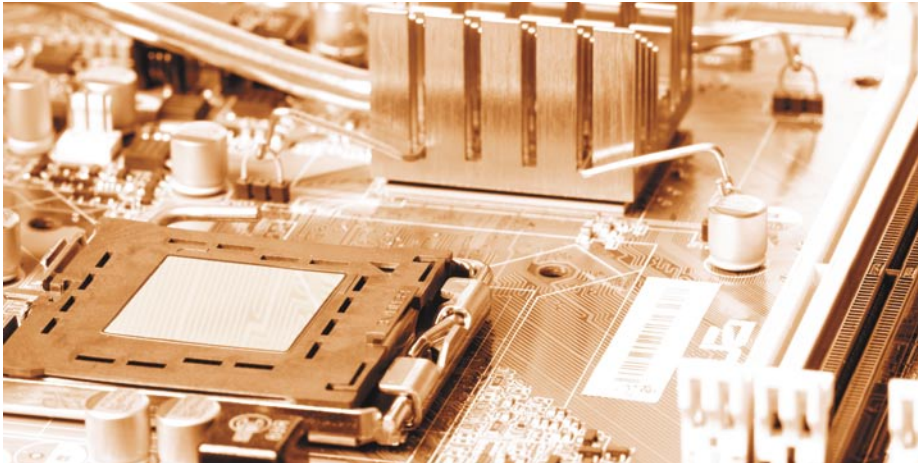


ESI Increasing value through effective ESI strategies

BY MUAZZIN MEHRBAN



The majority of Fortune 1000 and FTSE 100 companies are increasingly aware of their exposure to e-discovery ('e-disclosure' as it is more commonly known in the EU) risks – that is, risks associated with the use and storage of electronic data – and in response, have begun to employ internal solutions to address the issue. However, this process has been set back by the financial crisis, and many companies no longer have the resources to invest in protection against risks associated with electronically-stored information (ESI). In the US, the Federal Rules of Civil Procedure (which were amended in 2006), together with a number of high-profile cases, have served to help organisations realise their obligations to preserve and produce the necessary ESI in the event of litigation. But many companies have not paid enough attention to implementing ESI management strategies, making it difficult for them to respond to litigation in an efficient manner. Businesses need to have thorough records and information policies addressing ESI, as well as paper documents. Furthermore, all businesses which are regularly involved in litigation should have a dedicated, multi-disciplinary e-discovery response team.

Data danger

As a result of the staggering increase in data storage, IT departments have naturally come under huge pressure to reduce the associated risks. While electronic storage is cheaper and easier than ever before, the increasing volumes

of data must not only be stored, but also managed, accessed, secured and protected. The possibility of a company being involved in litigation adds an additional layer of complexity to this process. "Managing high volumes of data is a persistent issue because litigation hold requirements often result in the retention of data that would normally be destroyed in the ordinary course of business," explains Mark Yacano, a partner and leader of the Discovery Solutions Group at LeClairRyan. "Furthermore, headcounts, in both legal and IT departments, are shrinking, as well as the scope of managed IT services purchased by companies. There are significantly fewer people to assist with ESI-related issues and many of those people have other responsibilities for operating the business," he notes. Associated departments, such as information management and records management, are also operating under similar budget and personnel constraints. Further, in many respects, the processes used are not fit for all-purposes – IT departments are often forced to use systems designed for disaster recovery purposes, rather than electronic discovery.

Of course, these failings are well known in the corporate landscape – various legal and industry surveys have shown that companies are aware that they are not allocating sufficient time and resources towards effectively developing ESI strategies and policies. Somewhat paradoxically, the majority of these companies also realise the importance of ESI management, fully aware that litigation can over-

whelm a business and ruin its reputation. "The news headlines in the US are replete with stories of companies failing to manage, preserve and turn over ESI to government investigators or their litigation adversaries, resulting in substantial fines and monetary sanctions, as well as damage to their corporate image," says Stephen D. Whetstone, vice president of Client Development & Strategy at Stratify Inc. "Global companies in the UK and elsewhere are, now, increasingly under similar scrutiny, whether from various government regulators, the long arm jurisdiction of US authorities, or even local courts which, in the past year, have issued high-profile decisions concerning ESI lapses," he says. To avoid such scenarios, companies are advised to meet ESI challenges head on, prior to experiencing the fallout from a legal event, by which time it could be too late.

But clearly, on some level, businesses struggling to come to grips with ESI have failed to acknowledge the systemic risks attached to it. Indeed, with higher levels of digitally-stored data inevitably comes a need for more proactive management of ESI. Further, larger repositories of ESI often result in greater review costs. This can stretch an already small pool of IT-dedicated staff to the breaking point, leaving them less time to devote to other business functions. Maura R. Grossman, counsel at Wachtell, Lipton, Rosen & Katz, points out that companies which fail to adequately address ESI will find it increasingly difficult to sift through the masses of data when trying to find information for business purposes. "In the litigation context, processing and review of huge volumes of ESI have contributed to high discovery costs and missed deadlines, especially when active measures are not taken to assess and cull the data prior to attorney review for responsiveness and privilege," she warns.

The nature of these difficulties suggests that an e-discovery response team is probably the most efficient way to mitigate risks and reduce costs. Not only do such teams allow for institutional knowledge to develop over time, they also provide consistency and allow for preservation obligations and responses to information demands to be accomplished more smoothly. Also, and vitally, under no circumstances should a litigation crisis be the first time that a

company's legal team becomes familiar with its IT and records management departments. "The strategy a company takes depends, to some degree, on the size of the company," explains Mr Yacano. "Larger companies that are frequent litigants should consider enterprise level tools for the collection, filtering and searching of data prior to sending it for processing. Companies that lack those resources should develop strategic relationships with outside e-discovery counsel and vendors," he adds. Nonetheless, a multidimensional e-discovery response team can ensure a smoother and better coordinated response for most companies. A core group of personnel familiar with the company's IT systems, who know the location of relevant ESI, and whether ESI is readily accessible, is crucial.

A new approach

It is unfortunately the case that many companies fail to consider or dispose of an unwanted legacy data that exists, until an actual request for documents arrive. By that time, a company can often no longer discard them, as a duty to preserve duty may have triggered. As such, procedures which provide routine and well-intentioned destruction of ESI that is not subject to regulatory or other retention requirements can go a long way in both reducing the excessive volume of ESI, and protecting the business against spoliation sanctions. This, and indeed the whole approach to ESI, should start as soon as possible, and should be an ongoing effort. Company stakeholders should be prepared to conduct risk assessment analyses determining the size and scope of their data challenge, so that an appropriate and reasonable response can be devised. "The assessment should cover a variety of factors, including but not limited to the volume, type and scope of a company's prior legal cases and controversies, the amount of its past legal liability, the regulatory environment in which the company operates and the imposition of any specific records retention obligations, the company's size and complexity of its IT systems and applications, and the number of a company's facilities and their geographic locations," notes Mr Whetstone.

Thereafter, a company should have the basis to craft a document management policy which establishes basic rules concerning how long categories of ESI should be maintained. At this point, companies should also decide and publish the name of the persons responsible for record retention and litigation holds. Establishing this prior to litigation reduces confusion, and therefore the chance of mistakes during the first critical days after preservation duties are incurred. Perhaps the most important outcome to be learnt from an initial assessment is whether it is best to deal with such technical and legal challenges internally or otherwise. Indeed, by efficiently leveraging outside legal counsel and third-party consultants, companies can remove some of the risks from their own shoulders onto external experts, who can dedicate themselves to ESI management on a full-time basis.

However, protection comes at a cost, and the financial crisis has meant that many companies have had to tighten their budgets across many areas, including ESI. As such, it remains a challenge to convince organisations that, in spite of their financial difficulties, they must still be proactive in investing time and resources towards managing information. "The current financial crisis has only made that an even more difficult sell," agrees Ms Grossman. "There is also considerable resistance to adding the task of managing ESI to an already overburdened employee workforce. But failure to manage and control information at the front-end of the information lifecycle only leads to far greater burdens and costs when it needs to be located or produced, either for business or litigation purposes," she warns. Hence, there remains a strong case for adding resources to that effect even though it remains an uncertain time to deploy capital.

Of course, many companies, faced with spiralling ESI issues, have had no choice but to spend money, in spite of their financial situation. Ultimately, this is a wise investment, and will help companies to avoid serious litigation, which could have a terminal effect on their business. Times may be hard but companies are encouraged to create a lean, simple approach to

ESI management, given that ESI spend will become a fixed part of most companies' budgets, even in a downturn. Furthermore, the rapid changes in the way organisations and their staff communicate – even through social networking applications – has made it even more important for companies to remain up-to-date with the latest technologies used by their employees. "Information governance, including ESI management, should be adaptive. As the law and technology continue to develop, corporate legal and IT departments should follow the emerging and maturing technology to find ways to better manage volume and costs," asserts Mr Yacano. In response, many firms adopt end-to-end solutions, so that they can manage information throughout the entire data lifecycle – from the time it is created through to when it may be processed as part of a legal review. Mr Whetstone agrees, but stresses that external ESI-solutions, such as web hosted processing, review applications and data archives, often are better suited for the job, as they free up substantial capital that companies otherwise spend on upgrades, personnel and maintenance costs. "Companies that try to manage their ESI entirely in-house must purchase sufficient excess capacity and infrastructure, so they can try to cope with the inevitable, periodic spikes in data volumes and throughput. Of course, they also must carry the costs of that excess capacity when unused. On the other hand, by externalising data storage and processing costs, companies avoid paying for unused capacity and save substantial sums of money," he explains.

Keeping control of electronic information has been of increasing importance in recent years, but since the financial crisis, the risk profile has widened substantially. Consequently, managing the fallout from increasing litigation, increasingly complex IT infrastructures, widening threats to data security and harsher government regulations, while budgets are tight, is the new reality for most businesses. Ultimately, there is no substitute for thorough preparation, as it can help prevent costly mistakes, and better serve a corporation's ESI cost-savings and security. ■



Stephen D. Whetstone
VP Client Development & Strategy
T: 001 617 330 2828
E: swhetstone@stratify.com
www.stratify.com



Stephen D. Whetstone, Esq., is Stratify's Vice President, Client Development and Strategy and General Manager of Stratify's London and Boston offices.

Among other responsibilities, Stephen is charged with keeping abreast of legal developments affecting electronic discovery and disclosure, working with law firms and general counsel to craft document retention and discovery best practices, and honing Stratify's strategic position, services and product offerings in the legal market.

Prior to joining Stratify, Stephen was a litigation partner at Testa Hurwitz & Thibault, LLP, one of Boston's largest law firms, where for 11 years he represented clients in securities class actions,

government and internal investigations, patent and intellectual property matters, and other complex commercial litigation and at trial. Before joining Testa, Stephen was a litigator at Skadden.

While practicing, Stephen successfully handled many litigations and investigations that turned on analyzing large volumes of electronic data and evidence, often under daunting time constraints. His clients included Fortune 500 companies, leading international financial institutions, and publicly-traded and privately-held technology, pharmaceutical, and manufacturing companies. Stephen has written many articles and papers on electronic data, discovery and disclosure issues, which have appeared in the National Law Journal, Legal Times, IP Litigator, Privacy Law Journal,

Digital Discovery & E-Evidence, Industry Week, Mealey's, and other prominent international publications. He is also a frequent speaker at international conferences and CLE programs on electronic discovery and disclosure legal developments and best practices.

Stephen is a graduate of Bates College (B.A.) and Northeastern University School of Law (J.D.) and is admitted to the bar of Massachusetts, the U.S. District Court of Massachusetts, the U.S. Court of Appeals for the First Circuit, and the U.S. Court of Appeals for the Federal Circuit. Prior to law school, Stephen spent several years working in the political arena and with the media, including as Chief of Staff for Massachusetts State Senator (now U.S. Congressman) John W. Olver.