CORPORATE DISPUTES (UK)
JAN-MAR 2017(PRINT)

PERSPECTIVES

THE FUTURE OF E-DISCOVERY

BY **ADI ELLIOTT**
> EPIQ SYSTEMS

Electronic discovery (e-discovery) refers to any process in which electronically stored information (ESI) is sought, located, secured and searched with the intent of using it as evidence in a civil or criminal legal case. More recently, e-discovery has proved an invaluable tool when dealing with arbitrations, national and foreign regulatory investigations and internal investigations.

Organisations in the US and the UK in particular have been dealing with e-discovery for some time. But now that business transactions have become far more global in nature, companies in other countries also have to tackle e-discovery. In addition, there has been a rise in the number of regulatory investigations commenced by national and foreign regulators.

As we head into 2017, what are the key e-discovery challenges facing organisations and what can they do to ensure they are ready to respond?

Big Data

There are several aspects of modern working life that are making e-discovery increasingly complex. Data is erupting from email accounts, smartphones, tablets, social communities and search engines. Each employee is likely to send and receive multiple emails per day. And each email is likely to cross the desktops of dozens if not hundreds of individuals. That data is then archived and replicated and grows exponentially.

The sheer volume of data and the number of places in which it is stored complicates the e-discovery challenge.

Global business

As well as making e-discovery more important, the global nature of business is also making it more complex. And yet cross-border data transfers are not only frequent, but often crucial components of everyday business.

When it comes to retrieving and disclosing data, organisations need to make sure that they can do so without violating data transfer regulations and privacy laws. These risks are becoming more common as more countries implement privacy laws that regulate cross-border data transfers. Laws typically forbid cross-border transfers unless certain conditions are met or regulatory obligations are imposed upon the transferring companies.

Cost control

When assessing litigation costs, the number of documents that must be reviewed is a key consideration. Document review traditionally involves the reading (often at lawyers' hourly rates) of all documents which are deemed relevant to a legal matter. The potential litigation costs incurred by document review can be significantly reduced if organisations gain an early appreciation of the nature of their data, and are able to assess what is likely to be relevant to a regulatory investigation and

what can safely be removed from the data set prior to review.

An e-discovery specialist can help organisations establish an information governance process before litigation or a regulatory investigation arises. This process includes scoping systems and data that are potentially relevant to litigation, minimising exposure from unnecessary data. It is not enough to adopt an irregular pattern of data monitoring and leading organisations are recognising the benefit of adopting a proactive, continual approach to information governance. Partnering with expert e-discovery specialists at an early stage helps organisations to manage costs and avoid unplanned expenses.

Tackling timescales

In a constantly evolving panorama of national and international regulation and legislation, organisations, supported by their legal counsel, need to keep abreast of, and comply with, a complex range of rules and laws. Timeframes with which to respond to regulatory investigations can be strict and must be monitored.

For example, the EU General Data Protection Regulation, which will come into effect on 25 May 2018, will require organisations to report a data breach to the relevant authorities within 72 hours. In this instance, organisations will need to prove to the regulatory authorities that they had systems in place to minimise the risk of a breach in the first instance by demonstrating that they had established, well-communicated corporate policies as to data loss prevention and any associated auditing procedures.

They will also need to show that they had no advance knowledge of potential threats and that they responded with timely and adequate notice post-breach. In this context, an in-depth evaluation of the relevant communications is required. Utilising technology not only speeds up the response to data breach, but it also helps manage the cost of the exercise.

Technology in transition

The tools people use to communicate are changing, with greater focus on chat and social communication instead of traditional email communication. Accompanying these new communication types is a proliferation of apps such as Skype, Slack, Facebook, Twitter, HipChat, WeChat and Microsoft Teams to name a few. These 'short form' communications are increasingly where the

'thinking of an organisation resides' and they are establishing a whole new set of data streams.

At the same time, new technologies are coming to the e-discovery industry, too. For example, machine learning is making it easier to get to key data, as well as separating relevant data from non relevant data.

What are the different stages of e-discovery?

The first step is to identify where the data resides, as digital data is often on PCs, network files and email servers, smartphones, backup tapes and other storage devices. Investing the time to build a data map – essentially a description of the organisation's data types, technical infrastructure and storage solutions – is an important exercise, as this will show you where your data resides.

Once the dataset has been identified it will need to be culled, removing irrelevant employees, file types, junk mail and dates outside the scope of the investigation. It will then need to be searched using keywords that might help to find relevant documents. A good tool will also highlight those words in documents for easy review. Some tools will also provide a communications diagram, graphically showing the lines of communication between various parties on a particular topic. Email threading can also be helpful, as it lines up all the various email threads in a row, allowing the thread to be viewed in its entirety, rather than on a piecemeal basis.

After the relevant data has been identified the relevant documents will then need to be reviewed in order to build the case.

> "In order to ensure compliance, businesses need to make themselves e-discovery-ready across all countries in which they operate."

Are you e-discovery ready?

The world is changing. With the advent of smartphones and the cloud, the majority of documents created today are electronic and the bulk of these documents are never printed to paper. The consequential explosive growth of information and the rise of 'Big Data' means organisations face many complexities and increasing liabilities pertaining to their electronic discovery decisions.

Organisations cannot risk potential liabilities associated with the mismanagement of electronic data. In order to ensure compliance, businesses

need to make themselves e-discovery-ready across all countries in which they operate. Robust systems for capturing, categorising and retrieving key documents and data are necessary to ensure that information is rapidly retrievable regardless of type or location paving the way for a seamless e-discovery experience. CD

Adi Elliott
Vice President, Market Planning
Epiq Systems
T: +44 (0)207 367 9148
E: london@epiqsystems.co.uk