

DATA COLLECTION AND PROCESSING FOR LITIGATION



A CONTROL RISKS
CLIENT SURVEY



DATA COLLECTION AND PROCESSING FOR LITIGATION: A CONTROL RISKS CLIENT SURVEY

Background to the Research

Led by the Foreign Corrupt Practices Act in the US and the Bribery Act in the United Kingdom, there is now international anti-corruption regulation throughout the OECD outlawing organisations' use of corrupt practices both when they are doing business at home and abroad. In recent years, prosecutors have increasingly used the extra-territorial reach of anti-corruption legislation and co-ordinated their efforts in an effort to pursue major cases. The potential penalties for offences include prison sentences and punitive fines. Additionally, professional fees in investigating bribery can be substantial, and prosecution almost inevitably results in damage to the corporate brand.

Given this backdrop and the potential for senior legal executives to be held personally accountable for breaches of anti-corruption legislation, Control Risks conducted a survey of in-house legal teams to identify how they are responding to this greater threat.

Survey respondents came from the legal profession working for global organisations and held responsibilities covering litigation, counsel and electronic discovery. There were 50 responses to the survey. For clarity of reporting purposes, the statistics used throughout this study highlight the responses of those survey respondents expressing a firm position.



Key Findings

Pressures on the legal profession: regulatory concerns

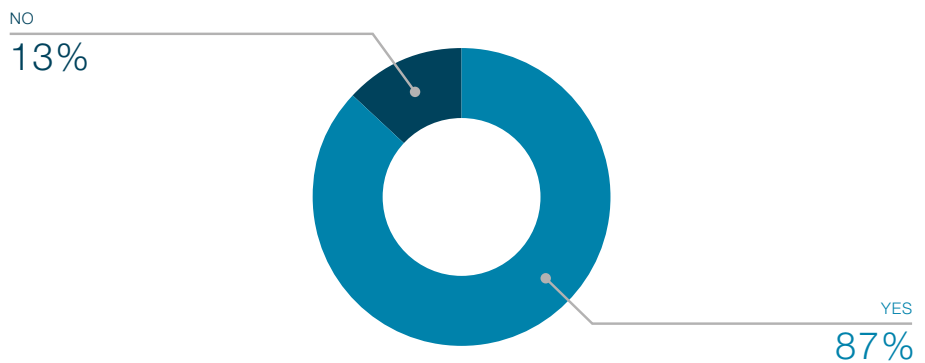
The survey first sought to understand more about the external factors impacting the legal profession and how these influenced our respondents' priorities. Regulatory pressure was a significant area of concern, with almost three quarters of respondents (72%) reporting increased scrutiny from regulatory bodies over the last year.

They were further asked about the preparedness of their own organisation. One in five of those surveyed (22%) had faced an issue in the past year which had resulted in an internal or regulatory investigation. In addition to the increasing regulatory burden and its tighter enforcement by regulators, factors such as an increase in whistleblowing also increased the risks to business. One third of respondents (39%) believed that their company was at greater risk of a regulatory request for information over the next 12 months compared to the previous year.

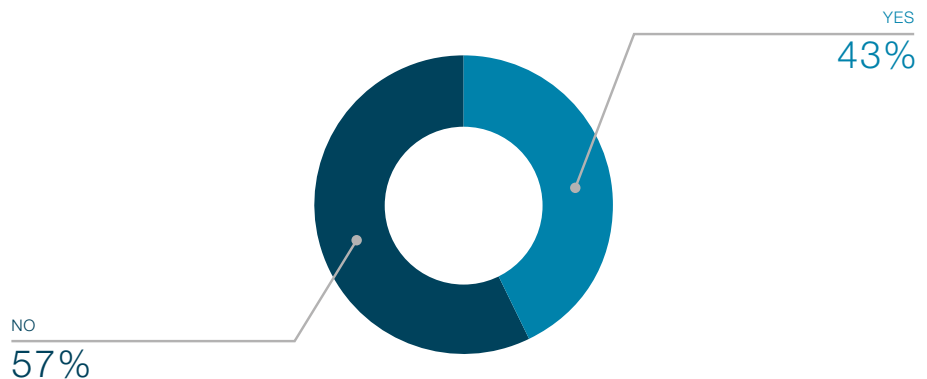
Managing Investigations

In-house legal teams are appropriately resourced to manage these regulatory and internal investigations, but many (43%) made regular use of outside counsel to support in conducting document review exercises.

Do you consider your in-house legal team to be of sufficient size and experience to manage internal or regulatory investigations?



Does your company make regular use of outside counsel to conduct document review exercises?

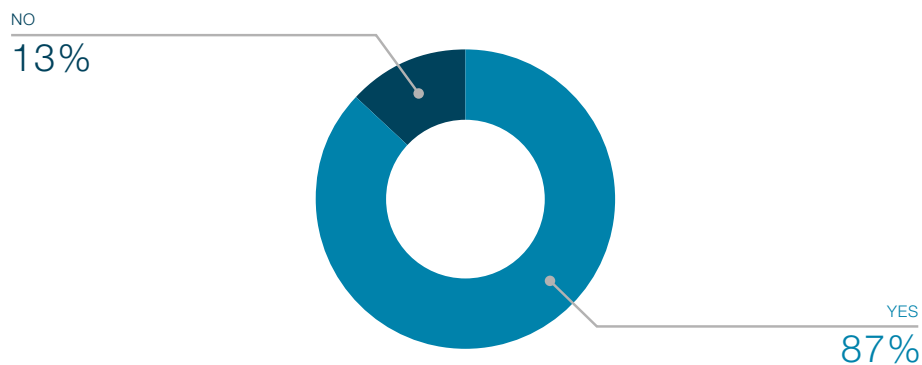




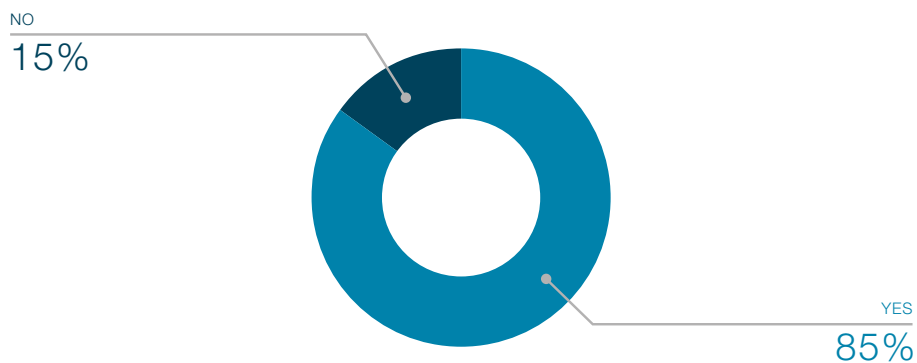
Managing Investigations: Data Retrieval

Legal counsels are adding new tools to their armoury to counter the increased threat, and the survey underlines the increasingly important role technology plays in this respect. Four fifths (87%) of all respondents felt technology had an important role to play in investigations and a similar proportion (85%) had engaged with an eDiscovery provider to help them both identify instances of malfeasance and, in the event of an investigation, to allow them to efficiently retrieve and sift through significant volumes of data quickly and cost-effectively.

Has your company considered the use of technology in order to cull data before involving outside counsel in any legal review?

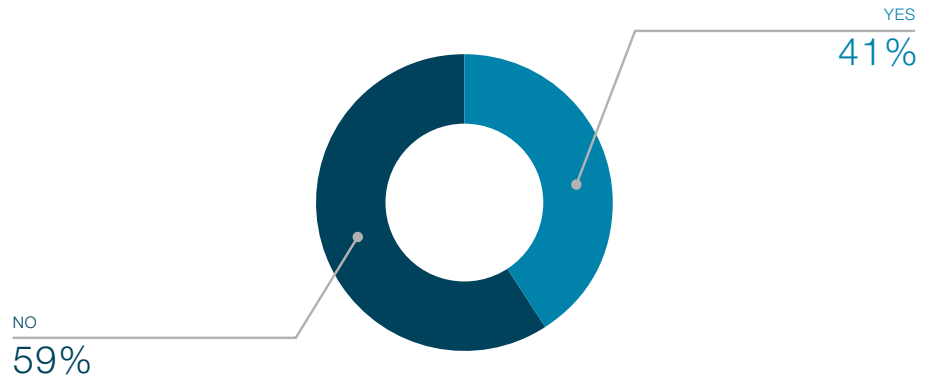


Does your company have a relationship with an eDiscovery provider?



Social media use by the business and its employees adds to the quantity of data produced. Whilst most respondents (59%) weren't overly concerned about social media usage within their organisation, they did recognise that this data could be used within an investigation (85% agree). 81% of respondent organisations had a social media policy to mitigate the risks.

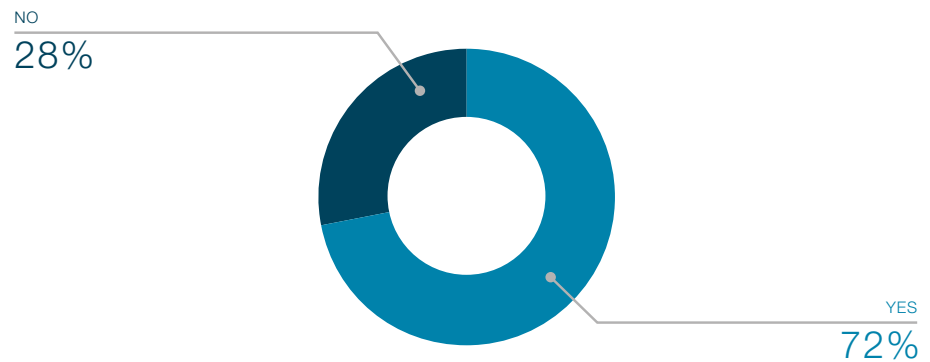
Are you concerned about social media usage within your organisation?



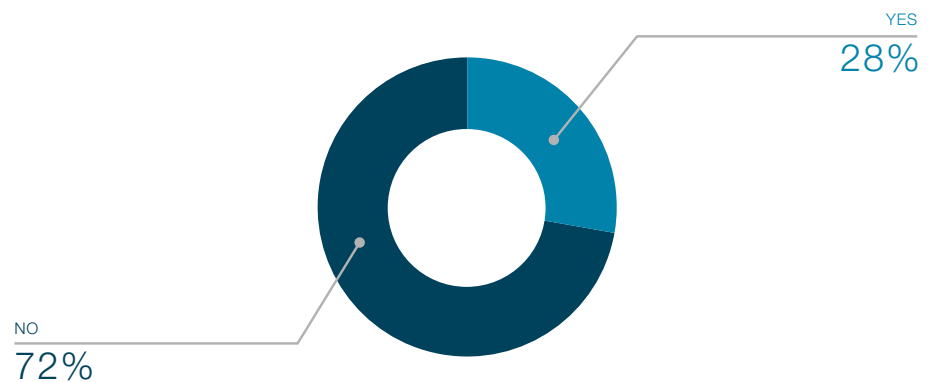
Data Storage

Whilst the legal profession is comfortable using the latest technology to retrieve data, data storage is a different matter. Most respondents (72%) backed up company information onto traditional tape media, but only one in four (28%) felt comfortable storing company information using a cloud-based data storage service.

Do you back up your data onto tape media?



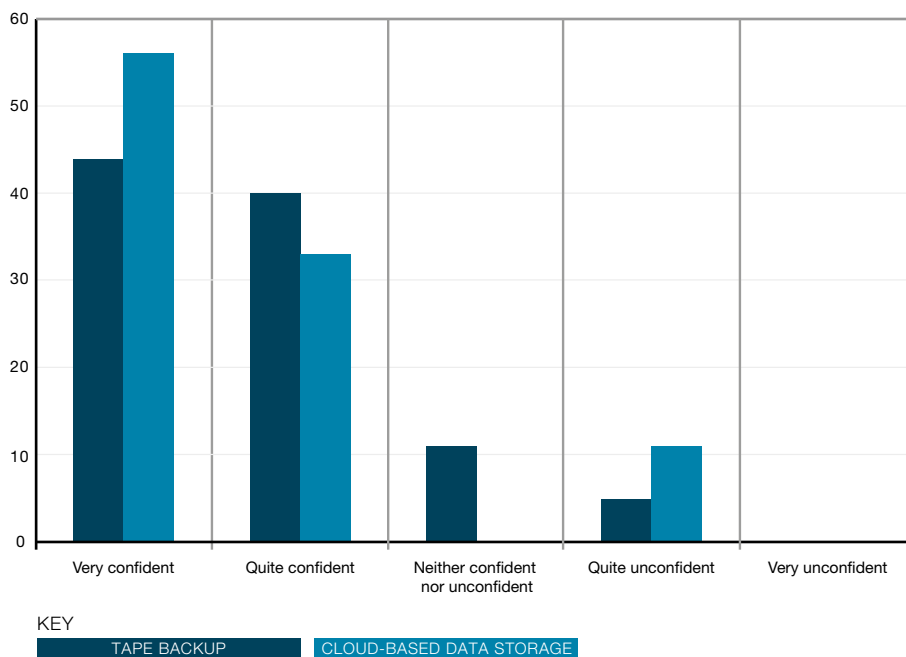
Do you store any company information with a cloud-based data storage service?





Whichever method respondents used for data storage, most (84% for tape, 89% for cloud-based) felt comfortable that information could be retrieved in the event of an investigation. Four fifths of respondents said they had formalised information retrieval plans in place to deal with such a scenario.

How confident are you that you can retrieve this data for investigative purposes? (percentage of respondents)



Managing Investigations: Data Analysis and Destruction

Businesses today produce vast volumes of data every day and whilst most organisations have plans and processes to retrieve this data, filtering and interpreting it to identify that which is relevant to an investigation can pose a more complex challenge. The experience of survey respondents, however, was that this was a more straightforward process.

Fewer than ten per cent (7%) felt that the measures implemented within their organisation would not be up to the task of analysing the data and pulling out information pertinent to the investigation, and indeed, two thirds (66%) of respondents had successfully retrieved data from cross-border locations or different jurisdictions in support of an internal or regulatory investigation.

Post investigation, four fifths (82%) of respondents said they had formal policies outlining how data should be destroyed within their organisation.



Implications for business

A clear conclusion from the findings of this survey is that in-house counsel is aware of the fact that they are facing increased scrutiny by international regulators. This is leading to many corporations strengthening their internal capabilities in order to both police and investigate potential regulatory incidents.

With the growing volumes of electronically stored information (ESI) across multiple sources, combined with the issues of storage and retrieval, investigations have inevitably become more complex. The challenge of retrieving and locating data in various locations is heightened by international data privacy laws. With this in mind, an increasing number of corporations are looking for independent, third party experts to assist them with either the legal expertise or technical solutions needed to examine the potential evidence.

One of the main messages from the survey is that eDiscovery technology and techniques are equally as crucial to business as legal know-how when it comes to regulatory investigations. In a more highly regulated environment, the challenge of being able to collect, filter and interpret efficiently increasingly large volumes of data is now being seen as a business critical requirement.

Control Risks' offices

abudhabi@controlrisks.com

alkhobar@controlrisks.com

algiers@controlrisks.com

amsterdam@controlrisks.com

baghdad@controlrisks.com

basra@controlrisks.com

beijing@controlrisks.com

berlin@controlrisks.com

bogota@controlrisks.com

copenhagen@controlrisks.com

delhi@controlrisks.com

dubai@controlrisks.com

erbil@controlrisks.com

hongkong@controlrisks.com

houston@controlrisks.com

islamabad@controlrisks.com

jakarta@controlrisks.com

johannesburg@controlrisks.com

lagos@controlrisks.com

london@controlrisks.com

losangeles@controlrisks.com

mexicocity@controlrisks.com

moscow@controlrisks.com

mumbai@controlrisks.com

newyork@controlrisks.com

panamacity@controlrisks.com

paris@controlrisks.com

saopaulo@controlrisks.com

shanghai@controlrisks.com

singapore@controlrisks.com

sydney@controlrisks.com

tokyo@controlrisks.com

washington@controlrisks.com

www.controlrisks.com