www.pwc.co.uk/edisclosure

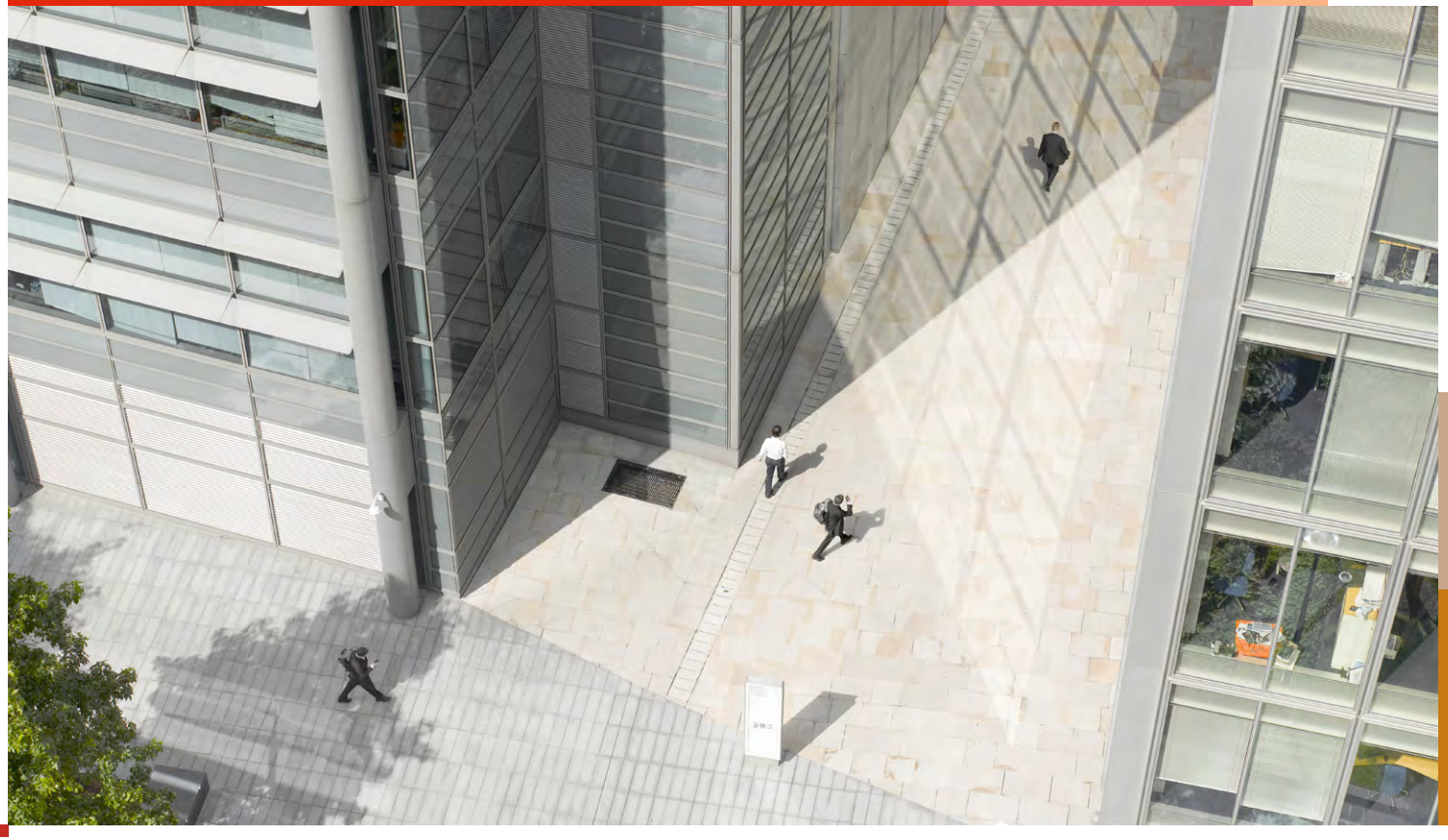
Click to launch

Creating a strategic framework for the future

e-Disclosure 2020

A report on the future of e-disclosure. Produced by PwC in association with

AKJ Associates



pwc

Critical trends are increasing the challenges of e-disclosure

Courts and regulators are becoming increasingly intolerant of ineffective e-disclosure.
There is considerable risk from regulators and courts who know that e-disclosure can be performed effectively and are not interested in hearing about challenges of preserving, searching and producing the right information. Sanctions and detrimental judgments are a real risk and can reach millions of pounds. This provides a compelling incentive for organisations to proactively implement good procedures and information governance.

Corporate data volumes grow upwards of 40% annually as they increase in complexity and variety.
Sources such as transactional data, instant messages, information from social networking and knowledge management sites, and audio and video recordings are driving increases in volume, complexity and variety. Without adequate prior preparation, this creates considerable disclosure challenges for organisations.

Storage capacity increases dramatically as costs plummet.
Every year, magnetic disk density doubles and flash drive capacity almost triples. The cost of storage falls and applications such as Gmail make users increasingly accustomed, both at work and at home, to storing all their information in perpetuity and recalling it on demand, without having to catalogue it in any way. Companies can face significant issues when this user behaviour meets inadequate corporate e-disclosure capabilities.

Outsourcing and cloud computing create new risks.
Driven by a combination of reduced costs, scalability, agility and redundancy, cloud computing is a matter of when, not if, for many large organisations. Driven by these benefits, organisations might not realise the significant risks beyond the commonly cited security issues. Organisations have less awareness of their data and less control over it, yet they retain the obligation to disclose it in a timely and cost-effective manner. They also retain the risk of penalties imposed if they are unable to do so.

To drive out costs, organisations are consolidating functions into shared service centres.
Local systems and the information they hold are being consolidated, often combining information from multiple countries and subject to differing regulations. The cost savings can be significant, but without proper planning they can complicate and delay disclosure proceedings, especially when multiple jurisdictions are involved.

Technological innovation is continuously changing the corporate information landscape.
New technologies are constantly introducing new data assets into the organisation, often before the associated risks and consequences are fully appreciated. Whereas technologies such as online banking had traditional counterparts for which the risk was understood, new developments like the iPhone and social networks have no risk benchmark. It is difficult to predict what new technologies are coming; it is even harder to predict their risks and impact. Organisations need a technology risk assessment framework to stay agile and adapt quickly to an unpredictable future.

The boundary between corporate and personal information is blurring.
New generations are entering the workplace seeking not so much to balance their life and work as integrate them. Values about privacy are shifting, as the change from privacy settings to "sociability" settings demonstrates. Professional networking sites, Twitter and other technologies allow quasi-corporate information to leave the organisation. Businesses must be aware of these risks and know how to manage them, especially if they contain content relevant to a legal dispute or regulatory matter.

Increasingly, litigation and regulatory matters span jurisdictions, subjecting companies to potentially conflicting regulations.
Keeping track of competing regulations at local and global levels is a challenge. Organisations have to manage their information sufficiently to meet the demands of a variety of regulations across multiple jurisdictions.

Technology brings innovations that can help solve these issues, but only if combined with strategies and processes to match.
As much as technology creates challenges with the exploding volume and new types of information, it is also a necessary part of the solution. Traditional methods for cataloguing and finding information are limited. New technologies are capable of vastly improving the way we search, group and review information, and they are the only way to manage exploding data volumes. Technologies to manage data on this scale must be implemented holistically, considering the lifecycle of technology adoption, and coupled with processes and policies to manage change and the adoption of new services.

Executive summary

Technological advances and soaring information volumes leave many organisations challenged to maintain information management strategies and manage the risks.

One consequence has been severe penalties for improper e-disclosure – the process of identifying and producing electronic information for litigation, investigation or regulatory purposes.

The technological and information explosion

Rapid and pervasive technological advancement is bringing new methods of communication and new types of electronic information that have no precedent and no counterpart in any traditional model. Communications, large and small, are sent so frequently that it is difficult to fully consider the consequences.

Organisations need to harness these advances in order to be effective, innovate, reduce costs and gain competitive advantage. They must, however, focus not only on the benefits of technology but also on the risk, regulatory and legal aspects.

e-Disclosure highlights the problems

The inherent urgency associated with a legal or regulatory requirement to disclose information can often focus attention on broader information management issues; these represent major potential risks capable of inflicting substantial financial and reputational damage on an organisation.

Doing it right this time

To help clients manage this growing risk we proposed a vision of e-disclosure and information management in 2020 derived from today's insights and experience. We challenged ourselves and our clients to imagine what the business and IT environment could be like in 2020. Then we talked about how to get there. We asked clients to picture themselves ten years from now looking back and ask: "What did we put in place and do well in 2010 to address the issues, opportunities and challenges we will face in 2020?"

By starting this conversation now we can help clients move away from a tactical response that merely contains the problem toward a strategic framework that helps to solve it.

"What did we put in place and do well in 2010 to address the issues, opportunities and challenges we will face in 2020?"

By starting this conversation now we can help clients move away from a tactical response that merely contains the problem toward a strategic framework that helps to solve it.

Good governance is key

One of the key insights from our findings is that it is important for organisations to assess their disclosure profile, perform a gap analysis and risk assessment, and remediate if appropriate. We call it e-disclosure governance.

At issue is the way that businesses manage the information they hold and manage the demands of stakeholders, regulators or counterparties to access that information. Good information management is central to effective e-disclosure.

The consequences of e-disclosure failures can be felt in the boardroom; resolution requires a broad business sponsorship rather than being viewed as merely an IT or legal issue. Contract risk with outsource providers was a major concern, as one panellist said, you can outsource your IT but you can't outsource your risk.

How to deal with the unpredictable

As to future threats, technology is often cited as the number one problem: it is responsible for the data deluge and each of its constant innovations creates new risks.

Our examination reveals that while technology is always a factor, it is only rarely the technology itself that is the problem. More often technology is an accelerator or catalyst, highlighting other underlying risk issues of information governance and individual behaviour.

This insight has two important benefits. First, we describe a technology risk assessment framework and recommend applying it to new technologies. This will identify the real risks – technological or not – and allow the organisation to focus attention there. Second, the framework addresses a rather thorny problem: if it is difficult to predict what new technologies are coming, it is doubly difficult to predict their risk and impact. Using this framework will increase organisational agility for managing the risk and adapting to unforeseen technological advances.

Hopes that technology will help solve the very problems that it creates are stymied by significant barriers to adoption. The most common methods used currently in e-disclosure, keyword searching and linear review, are increasingly ineffective for massive data volumes. More advanced capabilities show great promise, but the barriers to adopting them are practical, legal and philosophical more than technological. They are very real, pose inherent difficulties and will require attention and agility by all parties to overcome.

Take a holistic approach

Because of e-disclosure's legal connotation, some organisations have taken a narrow view, even dismissing it as simply an expensive and time-consuming exercise for legal and IT staff to solve.

Since the challenges inherent in e-disclosure come from the broader issues of information management, data governance and technological risk, so must the solutions be correspondingly broad and holistic. To successfully address e-disclosure, organisations must develop an approach that extends across all relevant departments within the enterprise. They must ask themselves "What information do we have? Why do we have it? How long do we keep it? When do we destroy it? When needed, can we preserve, protect, access, search and produce it?" And importantly, "What are the consequences if we cannot?"

Findings

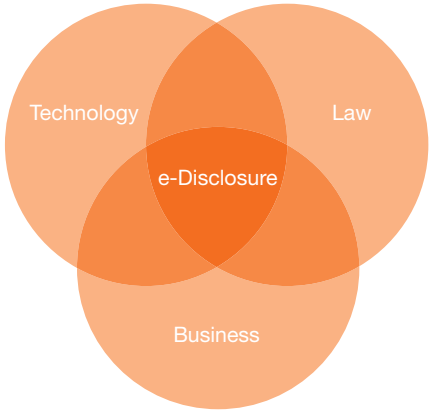
Legal issues were, as predicted, a major concern to panellists. There are questions as to whether e-disclosure regulations and the courts can keep up with the fast pace of change and new e-disclosure technologies. There is concern that global organisations will increasingly be caught between contradicting disclosure and data privacy regulations in different jurisdictions. There is also some uncertainty as to the future direction of regulations.

Navigating this environment will require substantial attention and innovation and organisations will have to take care not to get caught in the middle.

Less problematic than either technology or legal issues, the business concerns were focused mostly on balancing the need to adopt new technologies with the need to stay on top of the risks and potential consequences. A closely related point is anxiety over the people in the organisation: specifically how their use of technology and systems can be incompatible with information management and e-disclosure risk.

Conclusion

e-Disclosure brings together the three areas of technology, law and business. It provides the opportunity for organisations to examine the trends and risks across all three, responding with good e-disclosure governance and information management. Doing so will not only ease the pain, lower the cost and minimise the penalties of e-disclosure, it will also confer substantial benefits across the organisation, increasing business agility in a world ever dependent on massive volumes of electronic information.



Painful judgments and eye-watering fines

In this English case, "neither side paid attention to [the] advice" in the practice direction to "discuss issues that may arise regarding searches for electronic documents".

The judge ruled that the defendants "did not carry out an adequate search" and that they "acted unilaterally" not following the advice in the practice direction "as to cooperation with the other party" prior to the searches being done and the documents reviewed.

Result: Work worth £2 million in fees was ruled inadequate and had to be repeated.

In another English case, the judge wrote that it was "gross incompetence" for "those practicing in civil courts" not to know and practice the rules regarding e-disclosure.

The judge also wrote that "one expects [the party, a large corporation,] to have an efficient and effective information management system in place to provide identification, preservation, collection, processing, review analysis and production of its electronically-stored information…" and said that the "failure to disclose such critical information to assist the court is surprising and to be deplored".

The company was penalised with a reduction in costs because of their conduct before trial, which was "contrary to the overriding objective ensurng that the case is dealt with expeditiously and fairly."

Result: Defendant penalised by a reduction in costs.

(Continued on the next page.)

Painful judgments and eye-watering fines

(Continued from the previous page.)

In this American case, the court found that one of the parties intentionally "withheld tens of thousands of emails" and used the opposing party's "lack of access to the suppressed evidence to repeatedly and falsely aver that there was 'no evidence' ". Further, the company "has not presented any evidence attempting to explain or justify its failure to produce the documents".

The court found that the lawyers contributed to the "monumental discovery violation" and were "personally responsible".

Result: The company was ordered to pay over $8.5 million; the lawyers were named, sanctioned by the court, and referred to the state bar association for "investigation of possible ethical violations"; and both external and in-house lawyers were ordered to appear before the judge to develop a "comprehensive case review and enforcement of discovery obligations protocol".

This American case shows the monetary risk and reputational damage possible from improper e-discovery.

The judge wrote that "throughout this entire process, [the company] and its counsels' lack of candor has frustrated the court and opposing counsel's ability to be fully and timely informed." The failure to notify the opposing party and to process the tapes "was a wilful and gross abuse of its discovery obligations", its "failure to produce" emails and email attachments was "negligent" and its failure to "locate potentially responsive backup tapes" was "grossly negligent".

"By overwriting emails contrary to its legal obligation" the company "has spoiled evidence, justifying sanctions" and its "wilful disobedience…[also] justifies sanctions".

Result: The jury awarded damages of $1.5 billion. This award was later overturned, but on grounds unrelated to the discovery failures, and after considerable publicity and analysis of the case.

In an American case involving an individual and a large multinational corporation, the company was judged to have "failed to preserve relevant emails" and "acted wilfully in destroying potentially relevant information". It was charged the full costs of retrieving, restoring and validating all deleted e-mails and documents that were required during discovery.

Result: The organisation was fined $29 million and received considerable adverse publicity.

In this English criminal case a large prosecution was dropped after the presiding judge suggested that "manifest failures on the part of the prosecution are such as to render a fair trial impossible".

Result: Lengthy and complex prosecution aborted as the result of e-disclosure failures. In addition, the regulator is reconsidering the immunity from penalties originally granted to one of the parties.

Contents

A note on method

The findings in this paper have been gathered from a variety of sources including research and conversations with clients, lawyers and vendors. Bespoke research was conducted by AKJ Associates; it included an online survey of professionals from legal and technical backgrounds, the facilitation of roundtable discussions and an executive briefing at AKJ's annual e-disclosure conference. The survey ran from September 2009 to October 2009. The findings were drawn from 211 completed surveys. The results were also split by technical (124 responses) and legal (87 responses). The business roundtable discussion included in-house legal counsel, compliance, risk, IT specialists and technology experts from global FTSE 100 and FTSE 250 businesses; the legal roundtable hosted legal experts from global law firms, all of whom had in-depth knowledge of civil litigation, legal case trends and e-disclosure methodology.

PwC is grateful to its clients, the roundtable panellists, conference panellists, conference speakers, survey respondents, vendors, partners, staff and everyone else who has taken the time to be part of this discussion. Most discussions and interviews were conducted under the Chatham House rule, meaning that we may quote participants as long as we do not attribute the quote to the person or their organisation. Even though we are unable to thank the individuals and organisations by name, we are grateful for all their contributions.

Overview

Today's problems have limited solutions and are getting worse

Introducing a new perspective: e-disclosure governance

The journey so far

As corporate information moved from paper onto computers, paper disclosures became electronic ones, increasingly focused on e-mail and electronic files. e-Disclosure brought new issues that courts, lawyers and IT professionals had to deal with, including forensic data capture, metadata and deleted documents. Although disclosure has adapted to handle electronic data, the evolution from paper to electronic was merely incremental: e-disclosure was simply a modernisation of traditional disclosure. Even now the majority of disclosure consists fundamentally of documents – the memorandum has been replaced by e-mail, yet the two are inherently similar.

New technologies such as social networking and cloud computing have no traditional counterpart, yet are changing the business operating environment. If e-disclosure was difficult when electronic information was analogous to its paper predecessor, how will organisations manage with entirely new forms of information emerging today and the changes coming in the next ten years?

e-Disclosure 2020 set out to examine the future of e-disclosure in the context of technology, law and business by asking a number of questions. How can businesses further innovate and evolve to increase efficiency in e-disclosure processes and what benefits will arise as a consequence? In the future, what new and dynamic strategic functions are likely to become a necessity in order to reduce risk? What technologies might those functions be able to leverage to provide significant business value?

The symptom, not the disease

Many of the reports and assessments about e-disclosure have reached similar conclusions: as electronic information becomes easier to create and cheaper to store, data volumes rise inexorably. The costs of legal and technical processes related to e-disclosure rise quickly as a result. Eye-watering penalties and adverse judgments have been imposed on companies for getting e-disclosure wrong (see sidebar page 6).

"Clients don't know their own data, networks and systems, or where the data is located. There is poor categorisation of data and inconsistent taxonomy, resulting in inefficiency and needing more time to understand how information is stored and organised."

"Organisations have not prepared their IT infrastructures for data collection. The skill to extract and preserve is extremely rare."

e-Disclosure 2020 online survey respondents

These problems are simply high-profile symptoms of a wider difficulty with information management, a problem that is becoming progressively worse as business gets more complex and digital information grows more voluminous.

Getting it right is a weighty challenge and one that many organisations have not managed consistently and, more importantly, with a sustainable approach.

Papering over the cracks

The response is often a cycle of short-term fixes. Legal or regulatory action prompts a response to provide information. A tactical project handles the response. Some lessons are learnt that may improve procedures next time around, but these are improvements at the margin. Slow incremental progress in the face of oncoming transformational change will not do enough fast enough to ease the pain, reduce the cost and place information management on a sustainable platform for the future.

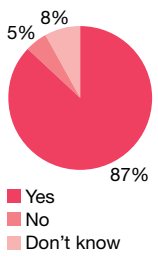
Technology torrent making it worse

Information management including e-disclosure will become much more difficult and will place additional stress on organisations already creaking under the strain. Technology is a major ratchet of this increasing pressure: fast-growing data volumes are overwhelming traditional strategies; challenging data types and formats, such as Excel spreadsheets, transactional data from enterprise systems and complex product databases are harder to manage; there is a growing use of voice recording, video recording and social media within businesses; handheld devices are increasingly connected, powerful and ubiquitous; and new technologies such as cloud computing are as necessary as they are misunderstood. All these, to name just a few, will drive greater complexity. How much is the future conspiring to make e-disclosure more difficult?

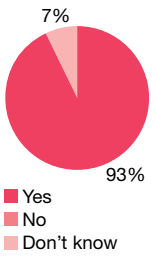
From the survey

From trends in cases [you have worked on for clients or you have observed in your organisation], do you believe that there will be an increased requirement to retrieve targeted data related to individuals, actions, or events?

Technical respondents



Legal respondents



Organisations becoming semi-permeable

The way that business is conducted will also continue to change dramatically. Employees are becoming increasingly mobile and location-independent and organisations more fluid. Some of the new generation entering the workplace are seeking not so much to balance their life and work as integrate them. Businesses' walls will continue to be opened and breached; the line between what is inside and what is outside – already blurring – will continue to become harder to discern and control. Demand for access to information will increase from stakeholders both inside and outside the organisation, from shareholders and business units to counterparties and regulators.

Opening access to systems

Consider how businesses have adapted to new technologies. The suggestion 30 years ago that banks and airlines should allow customer access to their computer systems would have been met with disbelief and horror. Today online banking and airline reservations are commonplace and have clear business benefits.

Managing information effectively, a necessary precursor to effective e-disclosure, is becoming increasingly difficult. Getting it right creates capabilities with broader benefits across the organisation. Getting it wrong will pose greater risks.

Pressure building

Organisations that do not understand and find an approach to address the problem will find themselves perpetually on the back foot trying to catch up. Meanwhile, risk, costs and complexity will keep rising. Attempts to make improvements solely for the short-term will be derailed by technology and business change. Courts and regulators will become increasingly intolerant of ineffective e-disclosure. The organisation's business units will be less patient about being unable to get the information they need when they need it.

"Archiving data is fine; trying to get it back out is a nightmare."

"We are great at putting things on to systems, not so great at getting them off."

e-Disclosure 2020 legal roundtable panellists

Developing a solution – one that is both robust enough to handle future demands and workable in the immediate and short term – urgently demands a new approach.

Fresh perspectives

Recognising this, we set out to build a vision of how data will be used and accessed in business and legal contexts now and in 2020 and how the legal community and regulators might see this new landscape. By starting now we can help organisations move away from using tactical responses that contain the problem and instead create a strategic framework for solving it.

The approach that we develop in this paper will enable businesses to identify the steps they need to take to achieve a dramatic influence on their information management capabilities. It will also help all parties to understand how judges and regulators might see the new landscape. Properly addressing these issues will not only help make e-disclosure easier, it will also help management of corporate information across the organisation.

We call it e-disclosure governance. Effective governance allows an organisation to respond quickly with agility to new developments. It means being able to adapt to the future. And because it offers flexibility and openness to both expected and unanticipated change, the governance-led approach can help to create an organisation that is future ready, whatever shape that future may take and whatever surprises it might contain. Getting this right will have significant additional benefits that flow far further across the organisation, going beyond satisfying the demands of counterparties or regulators.

In fact, a key insight we have drawn from our experience and research is quite the opposite: a governance-led approach is appropriate in most cases and will satisfy most organisations.

From the survey

When asked "What is the one thing you wish your clients/board would insist upon that would make responding to data requests easier in future?" survey respondents said:

- " That we implement a structured data storage process underpinned by indexing of stored documents."
- " Having adequate records management procedures in place."
- " An enterprise-wide data map."
- " Structuring data alike in the organisation."
- " Single point of responsibility for data governance, with that person having 'teeth'."

One size does fit all: e-disclosure governance defined

Not all organisations face the same challenges in managing and disclosing information. Some have relatively simple data universes which are well organised. Some are rarely involved in litigation and are subject only to minimal regulatory disclosures. Others have complex unorganised data, are more litigious and are subject to onerous and detailed specific regulatory disclosure.

These differences naturally led us to assume that creating a one-size-fits-all solution would prove impossible. Our expectations were that organisations' diverse regulatory, litigation, industry and information management profiles would lead us to develop different groups of recommendations for a variety of situations.

In fact, a key insight we have drawn from our experience and research is quite the opposite: a governance-led approach is appropriate in most cases and will satisfy most organisations.

e-Disclosure governance is a matter of

Assessing:

- what information the organisation holds, why it is held, how long it is kept, when it should be destroyed
- when needed, whether the organisation can
  - preserve, protect, access, search and produce the information
  - determine which portions of the information are relevant
  - disclose the relevant pieces of information without disclosing anything else
- the consequences if it cannot
- the nature, frequency, size and impact of disclosure requests facing the organisation (frequent or infrequent, large or small disclosures, large or small matters, regulatory or litigation, and so on).

Creating a gap analysis, action plan and governance framework.

From the survey

When asked to name risks created by the need to retrieve data which are not well understood, survey respondents said:

" Risk of damage to reputation if publicly criticised for not putting in place a defensible methodology."

" IT rarely has an understanding of why the information they have been tasked in collecting is of importance; [counsel] tends to restrict this information."

" IT doesn't understand the regulatory or legal requirements/consequences of storing data indefinitely."

" Sanctions that can be imposed by the court resulting in adverse judgments."

" Little forethought is given to how to get back to the data and the potential efficiencies of process/system designs."

Organisations that effectively implement e-disclosure governance will benefit from improved information risk management and greater organisational risk resilience.

Looking back from 2020, we would like to think that organisations will be able to identify the turning point when, prompted by e-disclosure issues, they decided to address information risk management as a whole. Today's short-term tactical approaches to e-disclosure have a silver lining – they expose the gaps between corporate functions and bring the organisational dependencies to the surface. This makes it easier to examine and rank the relevant risks, rather than just developing more complex ways of reacting.

Approaching e-disclosure and information management as a governance issue rather than a discrete technological or legal problem creates a number of opportunities. Identifying and prioritising e-disclosure risks provides a platform from which to build better information management policies and procedures that confer benefits across the organisation. It also offers key stakeholders such as chief information and compliance officers the opportunity to raise strategic information management as a senior management issue.

Furthermore, governance will supply the confidence that there are sound policies to support everyone in the business, indicators as to whether the policies are being followed and agility for adapting to changes at short notice.

This will require different functions to work together: we see internal audit, compliance and risk managers bringing their expertise to bear, helping the legal and IT departments to create, embed, manage and monitor policies across the organisation.

Organisations that effectively implement e-disclosure governance will benefit from improved information risk management and greater organisational risk resilience.

When we set out to examine the challenges and opportunities raised by information management, we split our enquiries between three main areas: technology, law and business. The following sections outline our findings, analyses and insights in each area.

Technology

As new technologies bring new innovations and benefits, they also raise new challenges and risks. For example, easy information creation and inexpensive storage appears long before tools to catalogue or sort that information.

New technologies and information types will always be developed and adopted well before the consequences and associated risks are understood.

If it is difficult to predict what new technologies are coming, it is doubly difficult to predict their risk and impact. We therefore suggest using a technology risk assessment framework to improve governance and organisational agility.

In March 2010 The Economist described the information technology changes coming in the next decade as a "technology avalanche". Rapid developments in IT are driving greater productivity and seemingly endless possibilities for collaboration and new ways of working within and between businesses. The proliferation of new types and sources of data make information management harder and the associated risks greater. Failure to manage information effectively can have wide and broadly damaging impacts; there is also the potential pain from the penalties associated with getting e-disclosure wrong (see sidebar: Painful judgments and eye-watering fines).

There is no standing still; the march of technology is relentless. Despite the risks and often unpredictable impacts, there is considerable pressure for organisations to adopt new technologies quickly. Outright bans or slow adoption processes are not realistic; they would stifle the innovation from which businesses gain benefits and competitive advantage.

The future is already here

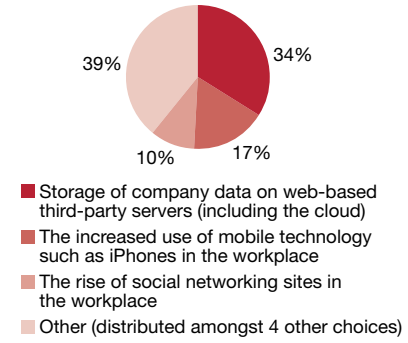
When we asked a range of IT and e-disclosure professionals which future technologies really concerned them, it was interesting that they chose cloud computing, mobile devices, social networking and Sharepoint, to name a few. It was even more interesting to realise that even though we asked about future technologies, all the major concerns cited were about technologies that are already in place.

"Tablet computing, holograms, interactive computer visualisation, instant messaging; those are what the developers are thinking. We are still thinking about some of the regulations."

e-Disclosure 2020 business roundtable panellist

From the survey

In terms of the ability and ease with which data can be retrieved, which of these technological trends is of the greatest concern to you?



How then to deal with the impact of technologies coming between now and 2020? At one point we envisioned a list of predictions of future technology with an analysis of the potential impacts from each (see sidebar: Some emerging and future technologies?). As with any list of predictions, it would include some that will come true and others that will not. Still other technologies not on the list will appear out of the blue and would have been missed from any analysis, limiting its usefulness.

To resolve the conundrum of managing unpredictable and unforeseeable risks, we took a different approach. After hearing what the concerns were, we analysed the largest perceived threats to understand why they caused concern. What was it about cloud computing and social networking that concerned people? What anxieties lay behind them? What does the technology change? What are the consequences? What are the risks? And why did respondents choose these and not other issues (such as data formats, transactional data, voice and video)?

Despite technology being commonly cited as the number one factor, our analysis reveals that while it is an ever-present factor, it is only sometimes the true cause of information management problems. Most of the time the technology acts to accelerate or highlight other issues.

Gauging the impacts

Moving data into an outsourced cloud, for example, relinquishes control over that data. Even if there are contractual arrangements in place to manage the data held in accordance with e-disclosure requirements – a big if according to some panellists – control over fulfilling that obligation is placed outside the organisation.

"…an off-record email system with business communication going out by the web over which the corporate owner has no knowledge or control whatsoever."

Contracting out the function does not mean that the risk is similarly devolved; as one panellist said, you can outsource your IT but you can't outsource your risk. Problems could range from the obvious – such as an outsource provider missing an important source of data – to the unexpected, such as the company whose outsource provider understood the disclosure request and had the means to deliver the data, but did not action it because they had no way to bill for that type of work.

From the survey

What are your concerns, if any, regarding privacy laws in cases that require data retrieval?

- "That the tension between legal requirements to disclose and the rights to privacy is not well enough understood within the organisation."
- "Company employees using their own private mobile phone handsets to send data."
- "Cloud storage that is not safe harbour or is located in the US."
- "Data protection and privacy requirements… are opaque and difficult (at best) to assess."
- "Contradictions in the law on personal data."
- "Cross jurisdictional data transfers, especially related to personal data and records being sent to the US."
- "Too many to list here."

Loss of control and data leakage emphatically came together when one client asked: "If the authorities seized a server in a cloud, what if it had my data on it too? What do the legal authorities have the right to ask for? Are there even relevant rules of evidence governing this?"

Social networking also carries the twin risks of data leakage and loss of control. Of the growing number of cases, one was as simple as an employee describing what work he liked doing thereby inadvertently disclosing corporate strategy. One panellist said that when he looked at how people were using the business networking site LinkedIn, he saw that it was "an off-record email system with business communication going out by the web over which the corporate owner has no knowledge or control whatsoever."

Others expressed similar concerns about systems such as Bloomberg and Reuters because of their email and instant messaging capabilities – however there is an important difference. As a client, the organisation would have a contractual relationship with Bloomberg and Reuters; we have, in a number of engagements, preserved or captured such messages. With social networking sites, content posted by individuals is governed by the agreement between the site and the individual. If an organisation needed content to be removed or disclosed, the relationship between the organisation and the site is ambiguous and is further confused by varying user agreements, privacy policies and acceptable use provisions.

"The next time we get an insider trading case and we find that knowledge leaped out of the organisation via LinkedIn or web mail, it is going to very dramatically change the space that we are working in.

e-Disclosure 2020 business roundtable panellist

Based on our analysis, we believe participants chose those particular technologies because of the true underlying risks: the inability to maintain control, the possibility of data leakage, the potential relevance to e-disclosure and the ease or difficulty with which information could be preserved, captured, accessed, searched and disclosed.

Moving for a better view

We therefore suggest a new way of looking at technology: a lens that provides a comprehensive and consistent assessment of the risks any new development creates.

Our approach provides a model for dealing with technology risks that cannot be seen, controlled or managed and limit an organisation's agility – its ability to manage and respond to new developments. This approach generates more insight and applies to any and all technological developments, predicted or unanticipated.

A new framework

We suggest looking at all emerging and future technological developments with these common themes:

- **Control:** what is the likely or potential loss of control that a new technology creates?
- **Data compromise:** what is the potential for information leakage?
- **Information awareness:** What is the likelihood that there would be information held or created by the new technology that would be needed by the organisation – either for its business purposes or for disclosure to a regulator or counterparty?
- **Accessibility:** How easy would it be to preserve, capture, access, search and disclose that information (and only the relevant information)?
- **Contract risk:** Does the arrangement give rise to contracting out the work without contracting out the risk? Like individuals who have responsibility without authority, organisations do not want to have legal obligations without the means to meet those obligations.
- **Legal uncertainty:** Does the technology raise issues for which there is no clear legal provision? What is the risk to the organisation of being a test case?
- **Context:** Will parties understand this information in context? One blogger complained that Twitter's 140-character limit made tweets impossible to understand, often requiring research into context only to find the tweets were irrelevant.

Using this new framework

By using this risk assessment approach it is possible for organisations to assess the likely impact on information management of any and all technologies. It also fits with overall governance, as we will see shortly, and increases organisational agility.

"In cases like the $1.5 billion judgment on back up tapes that were not found, I think there is a risk assessment missing about the potential for what I would call a 'black swan event'. After the fact it is obvious that it occurred, but most organisations are not anticipating how bad litigation can be."

e-Disclosure 2020 business roundtable panellist

To test this framework, consider a recent paradigm-shifting technology. One panellist said that 30 per cent of companies block access to Facebook. As soon as the iPhone came along, employees could once again access Facebook from their desks. Does this suddenly create an unacceptable risk? An organisation that had used a risk criteria framework would know the answer quickly, because they would have evaluated the underlying issue. Was blocking Facebook at the firewall done to prevent employees from socialising with friends during work hours? If so, it's more of a personnel and time management issue analogous to personal phone calls. If it was to prevent people from posting comments about their jobs, then it might be an attempt to prevent corporate information from leaving via an unauthorised route.

With a risk assessment framework, an organisation would look at the underlying risk issues and perhaps create acceptable use guidelines that become part of recurrent training or employee policy.

"What we have to do is try to keep one step ahead."

e-Disclosure 2020 business roundtable panellist

Again, using an approach based on risk criteria brings the essential problem to the surface. It is not the use of the technology per se that needs to be prevented, but rather the consequences that might come from its use.

Where technology reveals an underlying risk, it also points to the solution, such as policies, procedures and culture that guide behaviour.

"By the time businesses have got to grips with Twitter, the next thing will have come along…both in a planned way, with large organisations developing technology, down to home brew stuff which then takes off and gets used everywhere."

e-Disclosure 2020 legal roundtable panellist

Some emerging and potential future technologies?

- **Social networking:** Along with instant messaging, wikis and tweets, social networking is already becoming part of corporate communication. What are the implications on relevance, privacy, confidentiality and ownership of this information?
- **Cloud computing:** Servers and storage will move into the network cloud. The cloud can automatically move data from a full server to one with available space and move a processing job from a busy server to an idle one, anywhere on the globe. Which jurisdiction(s) apply to data that moves itself between countries? How might that affect data capture?
- **Tablet computing:** With the increasing use of tablet PCs as traditional notebooks, will organisations need to produce the electronic jottings of users in a similar fashion to the handwritten notebook?
- **Voice data:** Due to regulatory requirements, companies are increasingly forced to record telephone conversations. We must not forget that this information is still regarded as data and is subject to e-disclosure. The convergence of voice and data has been promised for a while, aided by technologies such as voice over IP. There are many services that now convert voice messages into text and vice versa. Are there implications to disclosing a message as text when it originated as a voice message?
- **Location-based services:** No longer limited to a car's navigation system, location-based services are now present in everything from mobile phones to memory cards for digital cameras. Will information sources such as these become more relevant and become discoverable?

(Continued on the next page.)

A basis for conversation

It seems natural for the IT function and the CIO in particular to engage in a productive dialogue with senior management about the information management risks facing their organisation. Even though many of the risks created by social networking or cloud computing are not technology problems *per se*, technology enables a change in behaviour that gives rise to new risks. The CIO has the ideal vantage point from which to spot these developments first and bring them to the organisation's attention.

> ***"A positive development to emerge from the financial crisis of 2008 was the realisation that risks are real and can happen to anyone."***
>
> e-Disclosure conference panellist

Building an information mandate

It is clear from the discussions that we have had with many e-disclosure professionals that there is an urgent need for businesses to understand the legal implications and impacts of a whole host of new technologies. Many thought the person in the best position to answer that need should be the CIO, emphasising the information component of their job title rather than their more familiar role of "managing the provision of IT".

The advances and changes that we can see coming are increasingly challenging; they demand a more informed dialogue that could help the CIO. One roundtable panellist described this opportunity when he said that by de-emphasising the operational aspects of managing the systems, cloud computing could give CIOs the ability to focus on managing information quality, policies and so on – elevating them from provisioning IT to managing information.

Some emerging and potential future technologies?

(Continued from the previous page.)

- **Servers in space:** Could jurisdictions create data centres that are neutral in location and difficult to reach? Is the way in which data is stored and transferred likely to involve more regulators and legislation? Taking the idea one step further, what are the implications of data servers orbiting in space?
- **Eye gaze tracking:** Cameras in the computer screen can track a user's gaze-point thus allowing an operator to interact with their environment using only their eyes. Might future disclosures include this tracking data, perhaps to prove that someone had actually read a document? Could biometric passwords be used to confirm an individual was actually using a computer at the time?
- **Three-dimensional holographic projections:** 3D holographic projections are a staple of science fiction and will probably be here eventually. Until then we have a massively growing body of unstructured data including recordings of telephone calls, conference calls, video conferences, web casts, boardroom TV and CCTV footage. Will we be able to search video for people whispering in corridors the way we can search audio recordings phonetically?

Lessons from information security

One panellist said that "a positive development to emerge from the financial crisis of 2008 was the realisation that risks are real and can happen to anyone". This heightened awareness means that there is more likely to be a receptive attitude to discussions about risk and a greater willingness to consider risks arising from previously overlooked sources. We suggest that in addressing information management risks it would be worth taking a look at how IT security is now assessed.

Years ago, new technology was introduced and the security holes plugged post-implementation; the chief information security officer (CISO) role did not exist. Today, the security implications of any new information technology are – or should be – rigorously assessed before they are allowed anywhere near a business's systems. We suggest that a light version of this now-standard approach could be used for e-disclosure. Organisations need to carry on embracing technology developments and should adopt an information risk assessment criteria that looks at the impact of technology on disclosure and information management risk. This should happen early in the adoption phase of new technologies, considering whether the information could be subject to disclosure and how easy or difficult it would be to preserve, capture, search and disclose.

Technology accelerates problems – can it also solve them?

If technology is contributing to the challenges then what part might it play in solving them? It is always easier to create and store information than it is to organise and catalogue it.

Technology to address the problem will help, but it is likely there will always be a gap. Ever hopeful, the majority of our survey respondents said that the most desirable development would be technology that could "recognise common themes emerging from disparate communications across different platforms or documents and link them together". Many organisations we talked to are also considering technology that could help with legal holds.

Ironically, the impediments to adopting such technology have so far been more legal than technological, as described in the next section.

Of less concern (for now)

"Audio can cost 80% more than email to process; it is the second most common form of evidence after email. Regulators love it."

e-Disclosure conference speaker

Perhaps surprisingly, different data types, such as video, audio and transactional data, were not perceived as particularly problematic, despite wide agreement that they are going to feature increasingly in e-disclosure. While the proliferation of video and audio content increases the size of the data files to be managed, the underlying information they contain appears to be viewed in much the same way as other documents – as a collection of words. We already conduct audio searches for clients, and if corporate video is mostly just meetings that are televised as part of a video-conferencing system, one could argue that word searching is still relevant. As to structured data, we already have tools for analysing financial transactions in a process analogous to document review. While these data types pose challenges, our sense from participants was that these were challenges that they could take in their stride, at least for the foreseeable future.

Law

As keyword searching and linear review struggle to scale effectively, massive information volumes can make e-disclosure increasingly expensive.

Technology – contributing to the problem through the information explosion – offers solutions, however there are practical barriers to adoption. This poses inherent difficulties and will require attention and agility by lawyers and judges to overcome. Addressing these issues will solve a problem that technology alone cannot.

Using e-disclosure tactics to gain advantage is well known and becoming less tolerated; there is growing sentiment that cooperation in e-disclosure is necessary and consistent with advocacy.

Courts and regulators are less tolerant of slow or improper e-disclosure and increasingly have the perception that it should be easy. Organisations will have to rise to that challenge.

Where technology is cited as the number one issue in the future of e-disclosure and information management, legal issues are a close second. Most concern is centred on e-disclosure regulations and the associated practice directions, although some people felt the regulations themselves were evergreen; it was the courts and the interpretations that were challenged to keep up. Also important is the overall legal and regulatory environment, along with new issues created by technology on which the law is silent or unclear.

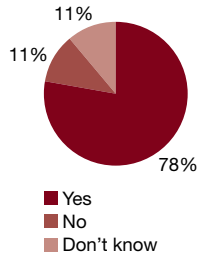
Both roundtable discussions identified discrepancies between the rules and reality. Some participants felt the rules were not keeping up, others simply that they were not being followed consistently. Everyone was concerned by the perceived danger of being caught between different regulations or standards. In some ways these issues are inherently more difficult than those discussed previously in the technology section. One very good illustration is keyword searching.

The end of the road for keywords? Where to turn next?

Panellists largely agreed that keyword searches are an imprecise tool for efficiently finding the relevant documents for e-disclosure. Said one panellist: “Even if you have a brilliant, absolutely focused search, you are still going to end up with too many documents to review and within those there will still be a very large proportion of irrelevant material.” One senior lawyer even said that “lawyers are not very good at creating search terms, but we think we are.” The consensus was that keyword searches are “a blunt instrument”. Regardless of the efficacy of keyword searching, data volumes alone are foretelling the end of keyword searching and linear document review. When data volumes are such that it would take hundreds of people many months to review all potentially relevant documents, it is clear that a better strategy is needed. As one of the panellists said, “In ten years it won’t be possible to just throw more reviewers at it.” Even today it is cost prohibitive in large matters.

From the survey

Would you agree that the main cause of inefficiency when trying to locate relevant data is that the methodology used returns a high volume of irrelevant records?



Respondents who answered "No" provided these alternative explanations:

- " Organisations have not prepared their IT infrastructures for data collection."
- " The volume or irrelevant records is certainly the primary problem… factors such as poor records management, a lack of understanding/expertise on the part of the client, failing to formulate a coherent strategy prior to collection, failing to adjust the strategy during collection and failing to focus the collection properly will all exacerbate the problem."
- " The client not knowing their own network and system, especially with regard to knowing where the data is located, and how many copies there are."
- " The way in which data and information is classified and retrieved."

"Poor search methodology will leave legal teams with a morass of data that is too large to reasonably review."

e-Disclosure conference speaker

Dark arts remain hidden

On the surface, help is at hand. More advanced search and review techniques include context- and concept-searching, automated document grouping, near de-duplication, email threading, predictive coding and data visualisation.

Various combinations of these techniques are becoming more common as part of investigations and early case assessment reviews, however there are barriers to their use in e-disclosure. The technological black box at the heart of these superior solutions creates uncertainty. While courts, regulators and opposing parties generally understand the outputs from keyword searches – and if not, it can be explained – advanced techniques are less well understood. Those same stakeholders have less assurance and confidence about what they are getting from advanced search technology. Delivering reassurance is a challenge.

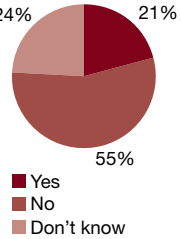
"I suspect that we will get to the point where judges really understand the concept of search terms and how they work and then we'll say 'Forget search terms, they aren't working we want to use this new software which does concept searching.' And the judge is going to say 'What! Enough already! You've just got us thinking about keyword searches and now you're going to throw this new thing on us?' "

e-Disclosure 2020 legal roundtable panellist

Progress is being made on a number of fronts. Some vendors suggest using advanced techniques to identify relevant documents and then using those documents to inform a list of appropriate keywords agreed by both parties, followed by a traditional keyword search on both sides. This is one way to address potential asymmetry that could be caused by only one side using advanced techniques. Others suggest using both advanced searching and keyword searching on a small sample of data and then comparing the results. When the advanced searches perform better for the sample (finding more relevant documents and fewer false positives) then parties will have confidence that the advanced search techniques can be trusted for the wider document population.

From the survey

Could advanced technology create a potential disadvantage "by decreasing the effort required by opposing counsel to locate evidence"?



The general sense from our discussions is that it is not the e-disclosure regulations themselves that need to keep up, but rather the practical application of those regulations to given cases; this largely falls to the individual parties, their counsel and the judges.

Some participants suggested that judges have only just understood keyword searching and would resist moving to advanced search methods, however there is light on the horizon. We are starting to see some courts suggest that keyword searching is inefficient and inaccurate, pushing litigants to try and use other more efficient methods for search and review.

In 2020 will we be looking back with incredulity, remembering the days when we relied solely on keyword searches? Almost certainly.

We are heading for an inevitable tipping point: as the effectiveness of keyword searches diminishes, there will be irresistible pressure to augment them with advanced search techniques. That pressure will build as data volumes increase and as advanced methods prove themselves.

Closely on the heels of advanced search techniques are advanced review capabilities. While advanced search improves the quality of the found document set, the documents still need to be reviewed. Using advanced search and then performing a manual linear review only solves half the problem. Automated document grouping and predictive coding techniques make document review more efficient by analysing the document population and providing sophisticated analyses to the reviewers.

We are heading for an inevitable tipping point: as the effectiveness of keyword searches diminishes, there will be irresistible pressure to augment them with advanced search techniques.

The same dynamics are at play; the pressure to use advanced review is increasing due to data volumes and the cost of manual review; likewise the courts and parties will need assurance that the results are reliable and in fact better than those from manual review, and we all have a role in making that happen as quickly as possible.

"It is a matter of individual judges who take an interest in the subject. We all know judges who are advocates of managing electronic information, who see the problems with cost and have the ability to give directions."

e-Disclosure 2020 legal roundtable panellist

How easy will it be to progress to that point from where we are today? It will depend on how quickly and adeptly we overcome the barriers to adopting these technologies. During this period of transition organisations and their counsel will have to stay abreast of these developments lest they find themselves squeezed between different approaches.

"Interactive visual interfaces are 'power tools for the brain'. They can reduce costs because they can quickly analyse patterns in massive data, helping us to be more effective at document review."

e-Disclosure conference speaker

Greater cooperation between opposing sides, or between the requesting and disclosing parties (with an emphasis on dialogue and iteration) may be called for. But this too could meet resistance, as lawyers involved in adversarial proceedings may be unwilling to spend more time cooperating than they have to.

The idea of cooperating adversaries sparked an interesting discussion at the legal roundtable, with one lawyer quoting a colleague who said that while the rules say one is obliged to cooperate with opposing counsel and work with them, "it is absolutely not to my advantage to work with them at all". Another suggested that in fact it was when it comes to e-disclosure.

Indeed, it is just that dichotomy that makes this area difficult. Litigation by its nature is adversarial; counsel has a duty to advocate for their client. It is our hope that this will not create an impediment to the adoption of new technology and advanced methods. Our thinking is echoed by our clients, various experts and industry groups. In short, parties should cooperate for the e-disclosure portion of the matter, because it is the only way to get to the evidence. Once parties have the evidence, they should be zealous advocates for their clients in arguing their cases based on that evidence. Lawyers we've spoken with say it has always been this way, and this argument is being made by the Sedona Conference's *Cooperation Proclamation*.

"[Parties] are pledging to reverse the legal culture of adversarial discovery that is driving up costs and delaying justice… by facilitating proportionality and cooperation in discovery…"

"Cooperation in discovery is consistent with zealous advocacy."

Sedona Conference

The challenge is to get parties to that point of cooperation to enable the best use of new technologies that will speed the process and lower the cost.

Will education help?

Panellists at both the corporate and legal roundtables talked about lawyers and judges becoming better informed about e-disclosure, citing leaders in the field. While this is a positive step, and is certainly useful for those who are contributing to the rules and practice directions, others questioned whether it is realistic to require this level of education from all judges and lawyers. One speaker suggested, given the challenge for technologists to keep up with the pace of technological change, that perhaps judges and lawyers had enough to do keeping up with changes in the law.

The smoking gun: reality or myth?

Questioning the need to obtain every single document, one panellist asked, "How many times do you ever find the smoking gun?" Another answered: "the smoking gun is a bit of a myth. In 20 years I have never found one. Most litigation depends not on finding the smoking gun, but building a picture of what happened based on what you can trace back. With email you have a commentary on what was happening in a way that ten years ago you would not have had. You have documents with dates and times, you can see who read them and who they were sent to. It is now possible to reconstruct the set of events much more closely than was ever the case before."

This prompted another panellist to raise proportionality, citing a case where "if we miss three documents, it is not going to matter, because there are hundreds of documents, they all deal with broadly the same thing. Those three documents will change the picture very slightly, but we are looking for the systemic view. How much did this happen? How regularly did it happen?"

Another panel member said: "It is not just about searching for one particular item; it is trying to extract from a mass of information what is pertinent and what is relevant. And that is becoming a real skill, which is not just a technology skill. I think that is a skill that lawyers perhaps have not developed in the way they maybe ought to have done during the last ten years." There are cases where judges have ordered considerable amounts of e-disclosure work to be repeated, at significant cost to the parties.

We then asked whether this might suggest a need for more flexible rules, allowing judges a choice. In the type of case where there could well be a smoking gun standards could be tighter, whereas if a smoking gun was unlikely, the process could be more proportional. Panellists liked the idea in principle but were unsure if it could work in practice. Said one lawyer, "I have a hard enough time dealing with one set of rules."

"What I am getting increasingly concerned about is the disconnect between what the rules require and what we do in practice. Practice is actually being driven by the technology capabilities more than the legal requirement."

e-Disclosure 2020 legal roundtable panellist

Regulatory requests: Computer! Show me everything!

We have stated that technological change can quickly outpace an organisation's ability to manage information effectively and that some organisations' current e-disclosure practices are lagging behind. If that is not bad enough, courts, regulators, opposing parties and indeed business users often have an accelerated view of what is possible in terms of finding information.

It is easy to see why. Some legal commentators have described something in American juries dubbed "the CSI effect". Driven by the popular television show, jurors' perceptions of forensic science have led them to believe that forensic evidence is quick, easy and incontrovertibly definitive. Likewise, roundtable participants felt there was considerable risk from regulators and courts who simply could not understand why preserving, searching and producing the right documents was really that difficult. One panellist said "we must think beyond traditional records management because the collecting net is cast very widely and the courts have expectations that corporations can produce it easily."

One conference speaker said that "courts think corporations possess a magic Google-esque portal" and can simply retrieve whatever information is needed.

A number of participants said that requests for regulatory disclosure were very broad; one said that the number of requests had almost doubled from the previous year. In addition, said another panellist, regulators routinely underestimated the cost of new regulation with regards to electronic documents and information. "While there is supposed to be an allowance for the cost of compliance built into regulation, in fact it is chewing up more and more resources."

Organisations have a choice: they can attempt to influence these perceptions, making the case that it is not as easy as everyone seems to think, or they can work towards meeting these expectations.

Also of concern to roundtable participants was simply that the less harmonised the regulations, the more discrete processes had to be created, each with its own costs. There was also disquiet expressed that organisations could get enmeshed by contradictions between regulations (disclosure and data protection for example) that varied across jurisdictions.

"The tension between legal requirements to disclose and the rights to privacy is not well enough understood within the organisation."

"Laws are not always clear and can be down to interpretation or misinterpretation."

"Keeping track of those laws at a global level in real time is a challenge."

e-Disclosure 2020 online survey respondents

"I've had two painful experiences where the judge basically said: 'you' (my client) 'are one of the largest companies in the world. You know the applicant in this matter is a single individual with limited resources. I am appalled to find that in terms of e-disclosure, this single guy seems to have done a better job than you have with all of your huge resources.' "

e-Disclosure 2020 legal roundtable panellist

US vs UK

In general, panellists and respondents are excited about bringing the best of the US across the pond and are not terribly worried about the problems. Opinion was universal that any progress in US courts' understanding of advanced search and accelerated review would be helpful here, as would efforts by industry groups.

From the survey

When asked "What are your concerns, if any, regarding privacy laws in cases that require data retrieval?" respondents said:

- "The tension between legal requirements to disclose and the rights to privacy is not well enough understood within the organisation."
- "Keeping track of those laws globally in real time and applying them against data at that time."
- "They are unclear, inconsistent and cannot be easily reconciled with US demands for data."
- "[The] inability to globally centralise e-disclosure operations due to differing privacy requirements around the world."
- "Multi-jurisdictional business such as ours will impose large number of potentially different obligations."

There was, as mentioned, concern about the burden of complying with multiple disparate regulatory environments. There was also concern that if the UK followed the US lead in e-discovery regulations regarding preservation, there was a risk of exploding volumes of satellite litigation.

"We understand fairly well what you are supposed to do when the action is up and running… the difficulty is as to what advice you should be giving to your clients when there is a prospect of litigation or dispute."

"In this country at this moment there is not a lot of case law which gives guidance as to preservation overall let alone electronic data."

e-Disclosure conference speakers

Of less concern (for now)

While prominent legal trends such as legal process outsourcing and third-party litigation funding have made headlines, they were not of significant concern to our respondents or panellists. We suggest this is because the risks and impacts are well understood. On legal process outsourcing the only comment was that it had to be managed well with appropriate contractual protections. Demand might decrease as advanced search techniques take off; however, it could be cyclical, increasing again when volumes explode until the next technological advance is developed and proven.

Though these were not of immediate concern to panellists, we of course recommend keeping these and other developments under review using the dynamic risk-based approach outlined earlier, as impacts could materialise in future.

"The global regulatory climate is not harmonized and in that sense it is impossible to follow all national legislation. It is difficult to understand the possible consequences in practice."

e-Disclosure 2020 online survey respondent

Business

Business needs can cause technology to be adopted before the consequences or risks are well understood. The risk analysis should be broader than technology itself to include behaviours enabled by the technology and impact on e-disclosure.

e-Disclosure should serve the business, not the other way around. e-Disclosure processes should sit across and connect all the relevant functional roles within the organisation.

Technology and e-disclosure create

People, that is to say business users, engage with new technology to create business advantages: cost reductions, competitive advantage, new offerings and so on. IT enables new ways to communicate – including blogging, tweeting, instant messaging, sharing tools, corporate wikis and social networking – giving people almost limitless ability to easily create a whole range of information-rich environments while the organisation has no way to control or catalogue what is stored where.

How people engage drives anxiety about unforeseeable consequences and impacts on managing information. These create risks to the organisation, including data leaking out or inappropriate content being created.

Anxiety arises from how some disruptive elements combine with the unpredictability of people. The single largest problem is people themselves acting – intentionally or not – in a way that takes no account of e-disclosure risk or information governance.

> "Systems aren't the main problem we face, it is people who use the systems – i.e., the end users everywhere in the business."
>
> e-Disclosure 2020 business roundtable panellist

Panellists were not optimistic that technology could help – for example by limiting the free-form ability to create emails with a mandatory system of controls. Business users would object to anything onerous, voluntary systems would have limited compliance, and in any event, such a solution would only work until the next disruptive technology came along.

Perfect systems, flawed users

Here again, technology needs to be evaluated: is it the root cause of the problem or simply an enabler of new behaviour? If the latter, it requires a correspondingly behaviour-driven approach to effectively diagnose and address its risk and impact. Again, the real issue is governance. Policies and education that can help people to understand the implications of their behaviour will create a far more sustainable solution for addressing information management risks than trying to impose increasing layers of technology on what may be accelerated by IT but is not in the end an IT problem.

Different users also change the risk picture. New entrants to the workforce can have a completely different attitude to their lives online than some of their older counterparts who have not grown up in a web-enabled world. That different world view can result in a different assessment of the risks of posting information online. They do not leave those attitudes at the door when they arrive at work.

Education, education, education

In much the same way that money laundering, bribery and corruption or other issues are addressed with training to instil the right behaviours and approach, setting the right tone from the top, it makes sense to treat information management in the same way. And as e-disclosure shines a light on broader information risk management issues, investing in appropriate training and raising awareness will help to generate a more robust approach that will have wider organisational benefits.

Making the right connections

Developing a governance-led approach to information risk management and e-disclosure raises the question of where responsibility for its execution should lie. At the moment in most organisations, as one panellist pointed out, "no-one is taking control"; no one person or group has responsibility.

"At the moment we are shooting arrows between silos in the corporation that each have well-defined processes and methodologies. Because people haven't done it before, it is always a new set of enquiries and a new type of investigation so it's easy to get it wrong. There is no established, articulated process. So if you were to think about drawing a process diagram, how you would do that, what would it look like?"

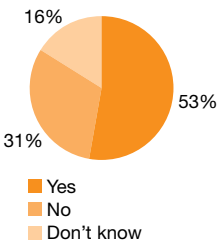
e-Disclosure 2020 business roundtable panellist

In our view, also expressed by roundtable participants, creating an e-disclosure function to address this would be the wrong approach. That is because the risk issues raised by e-disclosure and information management sit across a number of functions within the organisation. Any approach to addressing those risks should therefore sit across and connect a number of functional roles and responsibilities. Such a hybrid approach brings the most useful insights and know-how from a range of functions – not just IT and legal, but also risk management, compliance and internal audit – to help create an effective governance approach.

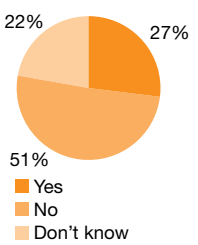
Effective disclosure is a joint responsibility.

From the survey

Do you believe that the need to retrieve electronic data in cases of litigation, investigations or regulation will necessitate the creation of a new strategic in-house function which manages all business processes that relate to data creation, storage, and retrieval in [your or your clients'] organisations?



Do [you or clients you work with] typically already have an operational function that manages one or more of the business processes mentioned above across the whole enterprise?



For example, one client that is taking this approach used their roles as information risk managers to form an interface between different parts of their business that need to know about e-disclosure. In their own words they are "translating, project managing and providing a single point of contact for legal, HR and compliance." This approach has also provided information about the business units that are making more requests for assistance than others and could provide valuable insights into bigger problems. If one business unit places a disproportionately high burden on the e-disclosure team, is it because their information is poorly managed relative to other business units? Perhaps it is because that business has a higher litigation profile. Would management benefit from having this kind of information and metrics? Might it allow different choices to be made?

"Something happens every five years and you don't spend any money on it. If it's trending up and happens three times a month, maybe you start."

e-Disclosure 2020 business roundtable panellist

In another example, an organisation has developed a policy to limit unrestricted access to networked storage and has instead created an approach that organises work into projects and all relevant information – including emails – are stored in that project location. While driven by the need to manage project information more effectively, it has clear benefits in terms of e-disclosure.

Conclusion

By adopting good e-disclosure governance and a technology risk assessment framework, organisations can lessen the risks and create a roadmap for the future.

The definition of e-disclosure, narrowly defined as part of a litigation or regulatory process, is no more. e-Disclosure is an information management issue, involving the identification, preservation, search, review and production of relevant corporate information to requesting parties, whether they are regulators, counterparties to litigation, stakeholders, or business units.

To be successful, organisations need to adopt a holistic approach, discarding the view of e-disclosure as purely a legal and IT matter. They need to address larger organisation-wide information management issues, involving functions across the organisation and with ownership from senior management.

With that solid foundation, organisations can prepare for the future by adopting a technology risk assessment framework and refreshing it regularly. All aspects we looked at – technology, business and law – tend to create challenges ahead of solving them. As new developments come along – only some of which are predictable – this framework will help the organisation manage its risk and maintain its agility.

Those with a responsibility for IT and e-disclosure will need to get close to the business and stay there. They'll also need to call attention to the risks that, because of their unique vantage point, only they can see. The organisation needs the agility to adapt to changing conditions and new developments, without being hamstrung by e-disclosure governance on the one hand and by introducing unknown or unacceptably high risks on the other.

In the one area where technology has the potential to significantly reduce the costs of e-disclosure – replacing keyword searches with advanced searching and replacing linear review with more automated review – the main obstacle is one of legal practice. Organisations, their counsel, the courts and regulators will have to work together to reap the promise of new technology, now and in the future.

A considerable amount of technological innovation will be required by all parties over the next ten years, and many organisations should be starting now.

When thought of in this context, the period from now until 2020 seems considerably shorter.

Recommendations

1. Senior management should take ownership of and responsibility for information management and e-disclosure governance. Heads of compliance, internal audit, IT, legal and risk should understand the risks and see that they are managed. Doing so will keep this off the board agenda, except perhaps as a "progressing well" status item rather than as a major crisis.

2. Organisations should be careful not to outsource control while retaining risk. While they will want to work with vendors and legal advisors, they can not abdicate responsibility to them.

3. Don't dismiss e-disclosure as simply a legal or IT issue. Take a holistic approach within the organisation to solving e-disclosure and information management.

4. Conduct an information audit to see what information you have and how organised it is. For financial services companies this can be tied in to efforts to create a "living will." Be sure to understand the difference between disaster recovery, backups and archives.

5. Assess your litigation, regulatory and business disclosure needs. Rank events with criteria such as high/low frequency, high/low impact, ease of responding, consequences of not responding, obstacles, and so on.

6. Use the attention paid to e-disclosure to:
   a. highlight which issues need to be fixed internally
   b. identify which technologies coming down the road indicate that action is needed elsewhere (for example, employee policy might need to be amended to deal with use of social networking sites)
   c. raise the issue to relevant parts of the organisation.

7. Conduct a gap analysis and create a phased remediation plan. If the budget for disclosure readiness is tight, consider slicing the remediation plan into small phases, so the work can be done on the back of:
   a. existing or incoming e-disclosure matters
   b. replacement or enhancement of archive, backup or disaster recovery systems or business continuity programmes
   c. routine efforts to refresh business continuity plans.

8. Determine which of the identified gaps create the biggest risks, and which would provide the largest number of early benefits, not just for e-disclosure but also for the business.

9. For e-disclosure work done before the remediation is complete, measure the costs and then estimate which costs would be lower and by how much if the remediation had been completed prior to the disclosure.

10. Define an appropriate framework or lens (as we outlined) for examining emerging and future technologies. Conduct your own risk assessment, remediate appropriately and refresh the lens regularly.

Contacts

Tom Lewis

Partner, Forensic Services
+44 20 7213 5911
tom.e.lewis@uk.pwc.com

Umang Paw

Director, Forensic Services
+44 20 7804 4347
umang.paw@uk.pwc.com

David Moloney

Director, Forensic Services
+44 20 7804 4262
david.r.moloney@uk.pwc.com

Russell Wallace

Director, Forensic Services
+44 113 289 4487
russell.l.wallace@uk.pwc.com

www.pwc.co.uk/edisclosure

Designed by studioec4 20286 (11/10)