Risk Management Considerations In Regard to Corporate Email and Electronic Documents

By Albert Kassis, Esq.
National Director, Esquire Litigation Solutions

A. Emails and electronic data (Electronically Stored Information-"ESI") are now integral to litigation and investigations

By now most risk managers are aware of the issues associated with emails, electronic documents, databases and records within their business environment. In legal circles and under the Federal Rules of Civil Procedure[1] these data fall under the legal classification of "Electronically Stored Information," herein known as "ESI." While these documents can be corporate assets they can also be corporate liabilities.

This article will address email, instant messaging, e-docs and the related risks that companies face in litigation and business. Additionally, this article will discuss what risk avoidance strategies and undertakings should take place.

Risk managers have likely thought of risks associated with electronic intruders from the outside getting access to corporate information. While still important, there is increasing danger which now comes from within the corporation- specifically the proliferation of electronic information that may create or provide evidence of liability. The trouble is that in the day to day activities of a corporation, liability is lurking and may never be uncovered until ESI shows up in a legal case or investigation. Previously both emails and electronic documents were discoverable, much like paper documents; the changes that took place in the Federal Rules of Civil Procedure on Dec 1, 2006 increase the level of awareness amongst attorneys in all practice groups. In fact, e-discovery practice groups and partners are now central in many law firms. Prior to the Federal Rule changes a number of litigating attorneys were of the "don't ask don't tell" mentality. What that means is if one side to a legal case didn't ask for emails to be turned over, then opposing counsel typically would do the same. Imagine that scenario now, particularly if a law firm or attorney loses a case. If ESI or particular ESI was never sought out and the non-requesting side loses the case, there may be some questions to answer to both a client and a Court in a potential malpractice claim. ESI really includes any information that is housed and can be retrieved electronically. This means documents referred

[1] See Cornell Web Site for E-Discovery, http://www.law.cornell.edu/rules/frcp/index.html

to above but also can include corporate databases, weblogs, voicemails, text messages and HTML files. It should be noted that it does not matter where the information is stored; This information can be on your servers, on backup tapes, on desktops, laptops and portable devices being used on and off site. Additionally, it can be content on your website or intranet.

Furthermore, the amended Federal Rules speed the process requiring litigants to turn over this material. The time period has been shortened to weeks in some instances. The risk associated with over or under capturing data to turn over is immense. To address these issues, risk managers can undertake activities and implement policies which will reduce the risks associated with these rules and other inherent hazards in the day to day business activity dealing with ESI.

Records Retention Policies

If your company does not have a records retention policy in place now, consider one as soon as feasible. The "Safe Harbor" of Federal Rule of Civil Procedure, Rule 37 safeguards an entity from *spoliation*- the intentional or negligent withholding, hiding or destruction of evidence or documents pursuant to a records retention policy. Specifically, 37(f) provides a safe harbor for litigants who fail to preserve ESI during normal business operations. This rule is designed to relieve entities from sanctions for the loss and or destruction of ESI as a result of routine, good faith operations of an electronic information system. This will allow companies to overwrite or delete older information to make way for new information. A collateral benefit will be costs savings associated with the possibility of reduced storage requirements. While the safe harbor works to offer some protection, it is limited. The records retention and "destruction" for that matter may be suspended. This occurs when a company has been provided a litigation hold or "preservation" letter or notice. Such a document requires an entity to preserve ESI and disable a records retention policy currently deleting information.

Records retention policies reduce risk in many ways. A properly crafted policy provides forethought to inhibit the accumulation of structured and unstructured data that can amass. Any accumulation that does take place will be done so for a legal reason or business purpose. All accumulating points- servers, desktops, and off-site locations, will be addressed. A map of those devices organizationally and their stake-holders is developed into a living document much like an organization chart. Key members are then assigned responsibilities to ensure that their portion of the map is kept up to date when changes occur. Any changes are discussed enterprise wide so as not to impact the policy of a different department. For example, if R&D would like to keep data longer than the HR department, both would work jointly to address any cross impact.

Some immediate steps can be taken prior to a formalized policy. Many corporations have adopted a form of a basic "time and space" policy for at least email. For example, emails that have been created and have existed for a period of time would provoke either a deletion or archiving response. The same would apply for data accumulation for a user. Regarding the "space" component, some employers address this issue by limiting the size of user's "in box." Once a threshold has been met you either have to archive your emails or the employee will not be able to

send or receive. Practically, employees would not keep 100,000 paper documents in their office without taking action. The same applies to electronic documents.

Related issues are whether different departments should have different retention policies. Also, are all the interested parties speaking to each other? IT typically is concerned about storage and retrieval issues. That department is not necessarily concerned about how these decisions may impact litigation their employer may be involved in. For those IT people knowledgeable about the litigation issues, they seem to be more inclined to work on short storage retention issues because such a policy may make them look guilty by appearance.

Archiving, a component of records retention, typically comes in the form of backup tapes. These tapes may retain previously deleted information, and are fair game with respect to an ESI, e-discovery request. The question however, becomes whether backup tapes are "reasonably accessible" under the Federal Rules,[2] and whether a corporate litigant should be subject to the expense of searching backup tapes.

Email Policies

1. Organizations should develop an email policy with input from each and every department, globally. This will benefit the organization's counsel, and will be instrumental in discovery requests.

2. Policies should include retention and usage as elaborated herein and should be reviewed annually. They should be more frequently reviewed when acquisitions happen, IT systems change and/or new software is implemented. Additionally, sensitive information relating to trade secrets, and attorney-client work-product need to be specifically addressed.

3. Policies need to be communicated and broadcasted, with face to face and departmental training sessions.

4. Policies should include "instant messaging" if relevant.

a) In regard to "instant messaging" (IM) within the workforce, the volume of usage has reached exponential growth. There are risks associated if the corporation takes a passive approach towards messaging. Some corporations allow their employees to use third-party messaging such as Yahoo. Non-company managed IM can create log trails on

[2] See FRCP Rule 26(b)(2)(B), Duty to Disclose: General Provisions Governing Discovery, http://www.law.cornell.edu/rules/frcp/Rule26.htm

corporate assets. Some of these logs can be stored on local hard drives causing headaches for any entity trying to respond to a discovery request while increasing risk that a trail exists unbeknownst to the organization.

Litigation Hold Issues

When organizations are sued, generally a preservation letter is sent from opposing counsel. It is the responsibility of the organization to then preserve all information embodied within the scope of this letter that deal with the litigation. The preservation obligation sometimes occurs before a letter actually is presented. If the entity has reason to believe they are going to be sued then the preservation obligation arises immediately. In both large and small organizations preservation should not be taken lightly. It has to be communicated to all those who are related to the litigation and who control the information embodied within the preservation letter.

The risk exists wherein someone does not get notice and deletes information that falls under the litigation hold. Risk managers need to work with both inside and outside counsel to assess how communications take place to implement holds. Communication regarding the hold has to be pervasive and re-occurring. Many corporations have established committees that deal with issues relating to these preservation holds and related matters. These committees come under a number of different descriptions including one that I have seen from time to time called "DART" which stands for "Discovery Action Response Team." This team is made up of a cross section of individuals. Depending on the organization, it may involve counsel, IT, and department heads.

Whether a corporation conducts a centralized or decentralized approach to preservation, their information "silos" will matter. Some DART teams involve departments including Sales, R&D and HR. DART teams are intended to implement a process and methodology toward responding to ESI requests in litigation. Related risk factors such as intrusions to business or work flow are necessary to anticipate. Both in response to litigation or a governmental "discovery" request, entities must be able to locate and review ESI no matter what the format may be and regardless of language.

Nuances abound that may inhibit locating relevant information, such as organizational changes in software applications or version. One can easily imagine the difficulties encountered by a corporation that switches from WordPerfect to Microsoft Word, for example. Additionally, if your organization has a records retention policy in place, routine overwriting of servers and data needs to cease. Special attention needs to be paid to servers that may "crash" and the resulting subsequent action taken, particularly if a preservation hold is in place or is expected. Also related are scenarios when new software is implemented and conversions of legacy data take place. Occasionally with hardware upgrades, relevant data may get moved to a temporary storage device which requires an update to any data map that the risk manager uses to monitor data silos.

From a business operations standpoint, litigation discovery holds are intrusive. They require affirmative action. The impact of preserving data for this hold on the day-to-day functions of your organization need to be addressed.

Further, litigation holds apply to those working both onsite and offsite. Employees need to understand what a hold is and what their subsequent actions should be. As a measure of assurance, some organizations require affirmative hold receipt notices whereby the employees acknowledge receipt of the hold and a log is created of all the affirmative responses. This helps to reduce risk and create a record of your efforts.

Both corporations and their employees are subject to this hold. While it is vital that a company understands its obligations under this hold, it is equally vital that employees do as well. In a recent District Court decision the court imposed a one million dollar fine after it concluded that spoliation took place when the company employees destroyed documents despite the corporation's efforts to preserve in accordance to Court order.[3]

Ultimately, whether a preservation hold was successful or not is tested by evidentiary production to the other side. Complete document productions will result in turning over all the relevant non-privileged documents. There have been numerous instances where all relevant emails have not been produced. Whether these occurrences are due to inadequate production holds is not always clear. Showing to a court that your organization has a well thought-out hold strategy helps thwart any spoliation charge. In some states spoliation is a separate civil action where a corporation can be held liable.

Having an email not show up in production has liability impact. Take for example the case of *Connor v. SunTrust Bank*, 2008 U.S. Dist. LEXIS 16917 (N.D. Ga. Mar. 5, 2008). In that case, the Plaintiff who had adopted a child, contended that removal of direct reports to her position and changes in her job responsibilities led to the eventual elimination of her job shortly after she returned to work. There was an email from plaintiff's supervisor which contained a statement that the position was eliminated due to the reduction from eight to three in the number of people supervised by her. This email copy was obtained by her from a source other than the employer-defendant who failed to produce this email in responding to her discovery requests. The Court held that plaintiff was prejudiced by the failure of SunTrust to produce the email. Specifically, this failure raised the question whether all other relevant email had been produced. The Court additionally noted that the defendant acted in bad faith. In the Court's opinion, the plaintiff's supervisor, who authored the email, must have affirmatively deleted the email from her sent items.

---

[3] See "*In re Prudential Insurance Company of America Sales Practice Litigation,* 169 F.R.D. 598 (D.N.J. 1997)

This example brings several issues to light, such as whether a properly implemented litigation hold may have prevented what had occurred in the SunTrust case. Could the hold have precluded deletion? From a software standpoint, it very well could have. Beyond software, a properly educated workforce could also have precluded any intentional deletion. SunTrust may never have known about the email. Both inside counsel and outside counsel to SunTrust were likely unaware because the supervisor may have been less than forthcoming and covered her tracks by deleting copies of the email and not telling attorneys handling this matter.

B. Steps to consider in protecting your organization from ESI risks

How would a risk manager protect their corporation from a scenario like the SunTrust case? There are certainly both liability issues and PR issues at hand.

Having properly executed records retention, email and litigation hold policies are necessary. While properly executed policies will assist in addressing some of these issues, they will not stop an employee trying to cover their tracks. If the employee knew that deleting an email from his/her sent box could be technologically uncovered, this may have thwarted their actions. Indeed many employees do not necessarily think or are aware of the intersection of litigation and technology as it relates to electronic documents.

It is vital for Risk Managers to ensure their employees are aware of the following:

1. Deleted emails and ESI can be recovered.
2. Date and time of deletion can be determined.
3. Employee internet activity can be traced.
4. Document "travel" from corporate environments to personal email can be traced.
5. ESI copied to remote devices (e.g. thumb drives or flash drives) or sent to printers is typically can easy to detect.
6. Voicemails could potentially also be retrieved and used for litigation.

Risk Managers with entities that are litigious in nature and find themselves in court frequently are in an advantageous position to work with counsel to safeguard against outcomes similar to the SunTrust matter. Safeguarding not only means litigation holds are properly executed, but that employees become more fluent in the hidden and not so hidden nuances of electronic documents and data. Consider it as part of the vital knowledge needed for corporations and employees to reduce overall risk. From an enterprise perspective, consider specific actions in regards to employees starting work at your business.

Have Your NEW Employees Been Schooled in the Following?

1. The policies of email communication within your corporation
2. The policies of email communication between your corporation and the outside world including business partners.

3. Informality traps of email and the legacy evidentiary issues that lie therein.
4. The binding effect of email that may occur in enforcing contracts and agreements.

Many corporations utilize different training and communication methods to get the message across. Some, for example, utilize their own employees to generate in-house training broadcasts. Podcasts that can be viewed at a user's workstation are ideal for those employees working remotely. These clips can also be used to educate employees on mandates such as litigation holds, email policies and inherent risks.

As noted above, email can have a binding effect. While emails can be perceived as informal in nature, they can satisfy the "Statute of Frauds" and create legally binding contracts. The case of *Al-Bawaba.com Inc. v. Nstein Techs.Corp.*[4] is an example where email had a binding effect. This case concerned a licensing agreement in which the sender had typed his name on the bottom of the email. The court held that "the sender manifested his intention to authenticate the e-mail for purposes of the Statute of Frauds by typing his name, 'Denis,' at the bottom of the January 12, 2007, e-mail referencing the parties' 'contractual agreement'".

So where the informality may be relied upon to easily facilitate communications, an employee may be able to bind a corporation in a contract merely by email. Additionally, for those employees that use work email to conduct personal business the binding effect of emails can also have impact in the personal affairs of employees. The implication is that any future enforcement of agreements or contracts by way of the binding effect of email can subject the employer's data and emails to discovery requests.

ESI Risks May Cause Negative Publicity

Negative public perceptions of your entity can develop from the mishandling of ESI during litigation. The core legal issues in the case can be superseded by the court focusing on one of the parties mishandling of the ESI. Some of the most highly publicized cases involving electronic discovery mishandling become synonymous with the corporation involved. Most recently the legal circles are buzzing about a case simply known as the "Qualcomm" case. In *Qualcomm Inc. v. Broadcom Corp.*[5] U.S. Magistrate Judge Barbara L. Major had sanctioned Qualcomm for "suppressing" over 40,000 electronic files. These files had been previously requested but did not show up in discovery. As it turns out, these files were dispositive but adversely to Qualcomm. In this scenario, Qualcomm's filing may not have taken place had these emails been uncovered prior to action being taken. A clear understanding, with policies and regimes adhered to, may have brought to light these emails at a juncture well before a filing may have taken place.

---

[4] See: *Al-Bawaba.com Inc. v. Nstein Techs. Corp.* No. 45550/07, 2008 N.Y. Slip Op. 50853(U), 2008 WL 1869751 (Sup. Ct. Kings Co. Apr. 25, 2008).

[5] See: *Qualcomm Inc. v. Broadcom Corp.* Case No. 05cv1958-B (BLM) (S.D. Calif. Jan. 7, 2008),

Another equally notorious case was the Morgan Stanley Case[6] which involved electronic data. On May 16, 2005, the Wall Street Journal published an article entitled, "How Morgan Stanley Botched a Big Case by Fumbling Emails." The merits of this matter were superseded with the negative PR associated with the ESI issues which led to the above headlines. In both examples, the case became synonymous with how the electronic evidence was mishandled.

C. ESI corporate policies should be communicated and reinforced

Regarding new and existing employees, you should be able to affirmatively answer the following questions:

1. Does your orientation program address employees' use of corporate systems and email use policies?
2. Are there training programs in place that address these issues for the continuing workforce?
3. Is there an "Acceptable ESI Use Policy" drafted, disseminated and communicated?
4. Are employees educated on the ramifications that emails can have on creating a binding contract, providing proof in litigation and generally on creating liability?

Imagine the overall benefits of creating, fostering and educating employees as to the above policies-particularly when specific examples were communicated such as the scenario that played out in the SunTrust case above. An employer's proactive approach would inhibit risk along many fronts.

Personnel-Employment Related ESI Risks

Use of emails as evidence in litigation is more common in legal actions related to personnel and employment matters. Emails have a unique impact on employee related claims against an employer or manager, as shown in the above referenced case, *Conor v. SunTrust Bank*, whereby the employee had copies of the email in hand which made it more difficult for the employer to prove that none existed.

Almost three-quarters of all litigation against corporations is employee related.[7] From a risk standpoint, employment related litigation is different from other forms, since the plaintiff-employee is actually part of the workforce. The communications between all the parties are embodied within the email and electronic document environment of the employer and can easily be moved to a third party email or printed as evidence that the communication happened.

[6] See: *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005

[7] See: Equal Employment Opportunity Commission Web site (www.eeoc.gov).

In *Zubalake v. UBS Warburg LLC*.[8], the plaintiff, Laura Zubalake, had copies of pertinent emails in hand. When those emails were not part of the production set, the Judge ordered backup tapes searched. In a number of these matters, Judges appear to impose a more stringent discovery requirement because the data is under the employer's control.

Exit Interviews as a Mechanism in Reducing Risk

Exit interviews are always of importance to employers. They allow for many things, including: insight on employees attitudes toward their former positions, toward supervisors and toward the general corporate environment. Equally important is to gauge whether an exiting employee intends to take legal action after leaving employment. This is important because various employers take action with data and emails previously within the exiting employee's control. For example, employers often "wipe" hard drives of exiting employees resulting in lost data. It is always best to wait to take action of this nature. An alternative would be to make a mirror copy or image of the hard drive if it is possible for the exiting employee to pursue litigation.

ESI as an Investigatory Asset

Companies now are subjected to a multitude of regulatory burdens. Consider the utilization of emails or e-docs in investigations as a mechanism to reduce risk. HR or Legal Counsel can search an employee's e-footprint to investigate issues relating to the following:

1. HR violations
2. Conduct in violation Sarbanes Oxley
3. Foreign Corrupt Practices Act
4. Securities and Exchange Commission issues
5. Trade Secret Misappropriation
6. Other various State and Federal Regulations

Consider that on a regular basis many individuals of high profile find themselves at the center of attention because of email communication. It has been once said, "why write when you can speak and why speak when you can whisper?" Let's face it -email from time to time has gotten companies and people into hot water. Consider Microsoft founder Bill Gates' emails introduced in support of the government's antitrust case. More recently, two hedge fund managers for Bear Stearns were taken into custody over roles they had in the collapse of their hedge funds. Ralph Cioffi and Matthew Tannin are facing criminal charges because in the email, Tannin allegedly said he was "afraid that the market for bond securities they had invested in was 'toast.'" According to the Wall

[8] See "*Zubulake v. UBS Warburg LLC*, 231 F.R.D. 159 (SDNY 2005)

Street Journal, he suggested shutting the funds. Several days later, though, the two managers told investors that they had comfort in the holdings of their funds.

The term "smoking gun" is used for emails that are clearly damaging to an entity or individual. Because email is treated much like chatting, often treated as private and unofficial, it is very susceptible to misinterpretation. A properly executed collection of ESI policies and procedures, continually reinforced would go a long way toward averting risk associated with the above example.

In May 2008, Forrester Research along with an email security company released a survey of more than 300 U.S. Companies.[9] The findings dealt with outbound security and email. The survey came up with the following findings:

- 34% of the companies surveyed had emails subpoenaed in the past year
- 26% of the companies terminated employees for violations in email policies
- 27% of the companies investigated a leak in sensitive information via a lost or stolen mobile device
- 41% of the large companies with more than 20,000 employees employ staff to monitor email.

The results are eye opening at the least. Consider the prospect that these percentages will only get higher given proliferation of these requests as permitted by the Federal Rules of Civil Procedure and soon to be a majority of the states who have adopted rules which emulate the Federal Rules.

Pro-Active Data Mining

Using ESI as an investigatory asset should be a precursor toward engaging in litigation. Many organizations are now hedging risk by mining data on their own servers prior to filing a lawsuit. This allows any unforeseen scenarios where smoking guns that may hinder a lawsuit are sought out prior to filing.

Technology and software has advanced which allows companies the ability of employing software that can automatically detect email policy violations. This technology can sequester risky emails all with the purpose of limiting liability. Most of these software applications have the same purpose and that is to prevent liability of one nature or another. Most implementations of software of this type involve establishing acceptable use policies. Some policies can include key words that are banned. These words are then programmed into the lexicon of the software that will then scan email messages. Also, some software allows for multiple lexicons for different business units. Some applications prevent mass emails which may be used in marketing. These types of emails may require disclaimers which would be required in certain industries. Software can also be used to

[9] See: http://www.proofpoint.com/id/outbound/index.php

prevent emails within certain departments of a company. This would potentially prevent theft of trade secrets or other information. One of the companies that provides this type of software is Messagegate Inc. This company has conducted use studies of emails, and some of the findings are of interest. In one such study, involving several sample sets of one million emails, and violations of acceptable use, the violations are worth noting:

- More than 50% of emails based on volume are non-business or inappropriate
- Up to 50% of in-bound company email by volume is non-business
- Social Security numbers were included in emails
- Emails contained racist remarks

Inherent Risk of Metadata within ESI

Metadata is defined as data about data. It is vital to ensure that your organization is aware of the risks associated with metadata.

Let's consider some of these risks. Documents leaving a corporate environment in their native applications can pose major risks. Microsoft's Word software has the ability to capture data behind the scenes which can create substantial risks. Specifically, the metadata captured and associated with a word document can reveal who the original author was and the date of the document's creation. Additionally, if a document is being drafted and a utility known as "track changes" is being used, all the revisions and comments between the parties are tracked and capable of being uncovered if the document remains in its native form and given to a third party. Consider some ramifications: an individual, who may be a customer or even competitor receiving the document can utilize their own software's "track changes" software to see what the sending parties changes were. They can also see if the sender was actually the creator of the document. They may also determine if this agreement was drafted for a different entity potentially seeing your company's other clients. They may gain advantage in seeing terms negotiated for other clients that are not part of the terms of the agreement within their hands. Private and confidential information may be made public.

Two publicized metadata snafus involve the following:

1. During the nomination process of Judge Alito to the Supreme Court, the Democratic National Committee put out a memorandum criticizing his nomination. This document was disseminated in its native form. It was later discovered through the metadata that the document was written well before the Judge's nomination.

2. An announcement by the Law Firm Bois Schiller on a lawsuit revealed a potential future defendant whose identity the firm wanted to keep private.

Many corporations require that documents leaving an electronic environment of an organization have to do so in a static or petrified "image format." For the most part, Adobe's PDF format accomplishes this.

Other ESI risks may come about by human error. Some email software has an "auto look up" or "auto-fill" feature that allows for frequently used email addresses to be inserted within an email "send line." Consider a recent scenario that happened with an Eli Lilly in-house attorney who was working on a very large settlement. In an email full of company sensitive information, which included information on a fine to be paid, the in-house attorney inadvertently sent the email to a New York Times reporter instead of outside counsel. The reporter had a similar last name to the intended recipient and the auto-fill email feature in the email software substituted the wrong name for the right one. News of the email became widespread soon thereafter.

Strategies with Service Partners Help Reduce Risk

In years past when corporations were involved in litigation they looked to their outside counsel typically to make decisions on which service partners to use to support the efforts of counsel. Risks were nominal in that information, particularly electronic, was confined and not of the same significance as today. With the paradigm change, service partners are of critical importance. A particular decision on a service partner can increase or decrease the risks associated with ESI. Equally important are the costs associated with the service partner decisions.

Currently the environment is changing in that corporations are formalizing internally what service partners to use and imposing those decisions on outside counsel. The risk reduction benefits are as follows:

- Corporations are establishing formal service partner RFPs with this tailored toward their specific needs, architecture and workflow
- Inside and Outside Counsel are collaborating to establish RFP requirements that cause overall efficiencies
- Workflows are recognized. Selected service providers understand their clients, and maximize knowledge to handle ESI
- Service providers that realize they can get significant business from a corporate client can establish business practices that conform to the corporate client, including specific billing procedures
- Down time associated with training and interacting with law firm selected service partners are kept at a minimum
- Legal technology causing efficiencies can be collaborated more appropriately with the corporations IT staff resulting in benefits to a number of departments
- ESI technologies associated with flagging and indexing work product and privileged ESI can be integrated resulting in less risk of those documents being released in a litigation production despite counsel protections to the contrary

Enterprise E-Discovery ESI Solutions

While selecting service partners is beneficial, it may not make total sense all the time. Some companies and industries are more prone and knee deep with all the issues associated with this article. If the issues raised are routine and part of the day to day existence of the corporation, risk managers need to possibly seek out enterprise solutions for many of these hazards. Now is the time to consider making such a move since the data is growing at an exponential rate. While outsourcing

some of these tasks makes sense in organizations with infrequent litigation it doesn't make sense with those entities in court on a weekly basis. The software by Messagegate Inc., as referred to above provides a component of the enterprise solution. Other applications provide other components of the solution. These applications include:

1. Litigation hold software that isolates relevant custodian data for preservation purposes
2. Data architecture software, which maps and updates data silo's and stakeholders
3. Software that isolates, collects and harvests globally across an enterprise's data pursuant to a discovery request
4. Evidence review applications that streamlines review of data

Corporate Insurance Implications

Insurance companies are taking a hard look toward covering companies from liability in discovery costs associated with ESI. Some insurance companies are mandating training programs or requiring exclusions. Several insurance companies have adapted to this risk associated with ESI and have generated specific electronic discovery insurance coverage that provides some degree of protection in this regard. There are ancillary benefits of this coverage. In conjunction with the company writing a policy, typically the ESI welfare and structure is audited which assists risk managers in uncovering weaknesses and addressing shortcomings. Chubb Group, for example has issued publications meant to assist clients. They have provided publications and advice on records management and issues relating to ESI.[10] Insurance companies are in a unique position of overseeing this process in that they are commonly both litigant and underwriter. In that regard they likely will be a best practices resource for some time to come.

Conclusion

The proliferation of electronic data and the current habits of the workforce at times collide, creating risk increases. As it relates to ESI, Risk Managers face a similar role to Safety Officers. Best practices must be communicated, monitored and sanctioned if violations have occurred. The education, monitoring and continual reinforcement of ESI policies will lead to a decrease in risk, enterprise wide. The business community has recognized this risk. Technologies are being developed to help increase management of ESI and curb activity which would be adverse to ESI management.

[10] See, Loss Prevention Resources, The Chubb Corp., at www.chubb.com/businesses/chubb3331.html