ASSOCIATION OF CORPORATE COUNSEL

TITLE: **eDiscovery 911! Building a Discovery Response Team for Effective Legal Hold Management**

DATE: **August 26th, 2008**

PRESENTED BY: **ACC's Litigation Committee**

SPONSORED BY: **Covington & Burling, LLP**

FACULTY: **Ben Hawksworth**, Senior Manager, Ernst & Young
David Wetmore, Executive Director, Ernst & Young

MODERATOR: **Monica Palko,** Associate Corporate Counsel – Litigation, BearingPoint

****

Operator: Welcome to this ACC webcast. Monica, please go ahead.

Monica Palko: Hello, everyone, and an additional welcome from us to the eDiscovery 911 presentation, building a response team for effective legal hold management. Today's focus is a proactive one. It's about building a cross-functional team to implement and manage legal holds, so we'll talk about how e-discovery response teams are established and structured, the role of the team and techniques for effective hold management.

And before we get started, I'd like to introduce the team. I'm Monica Palko. I'll be the moderator and the in-house panelist today. I'm Associate Corporate Counsel for Litigation with BearingPoint. Prior to coming to BearingPoint about five years ago, I was a trial attorney in the commercial litigation branch of the Department of Justice in Washington, D.C., and before that I was in private practice at was then Bracewell & Patterson. Now it's Bracewell & Giuliani.

I am very pleased to introduce our distinguished speakers from Ernst & Young. As most of you know Ernst & Young is the Litigation Committee's sponsor and we're very fortunate to have them. David and Ben, David Wetmore and Ben Hawksworth, our speakers today, drafted the info pack, which you'll see on the left side of your screen. It's item number five, implementing legal holds.

And it was actually quite a task for us to take that extensive info pack and choose one topic to discuss on the webcast today, and I think we did a good job of that. But I do want to refer every to the info pack, which is an excellent resource.

So David Wetmore is an Executive Director with Ernst & Young, and he leads the delivery of discovery services there. He assists clients with designing comprehensive discovery response programs and he also frequently assists with designing and implementing legal holds and developing inventories of inaccessible ESI media. He also leads teams in the delivery of forensic technology services in support of internal investigations and litigation.

Ben Hawksworth is a Senior Manager at Ernst & Young, where he works on discovery advisory and discovery services engagements. He focuses on legal technology services, including discovery response risk assessments, legal hold effectiveness assessments, legal hold design and implementation, also the processing of electronic information and discovery management advisory services.

So we would like this to be as interactive as possible, recognizing that we're all sitting at different computers. We will try to let you know who is speaking, but in case we don't, I'll give you a shorthand. You'll recognize Ben’s voice because he has the British accent. I'm the only girl, and David's the other one.

So a few announcements, just logistically before we actually get into the substance of the program. You can ask a question by typing it into the box in the lower left-hand corner of your screen. I want to be very clear that the questions are completely anonymous, so don't be shy to ask them. I won't be able to see your e-mail address or any identifying information. And we really do encourage you to go ahead and ask some questions today.

It helps if you keep them somewhat short. It can be a little bit tough to read a lot of background. We've also incorporated what are called some polling questions into our presentation and when we get to a polling slide, you'll actually be able to tick a box on your screen to answer the question. Your response will be completely anonymous, again, but everyone will see sort of a percentage response.

For example, 50 percent of people prefer a Big Mac, that sort of thing. And then finally a reminder to please complete the webcast evaluation form, which is item number six on the list of documents on the left-hand side. We will read all of those evaluations. We value them very much in terms of improving the program. That's also a good thing to do if by chance we don't get to your question or maybe you have a question you would like to address to Ernst & Young privately, you can complete that form and send it in and that will be delivered to Ernst & Young.

So let's get started. We're going to start it off with a polling slide, so you'll be able to tick right on your screen if you see the slide, what's your level of experience with today's topic? We're asking this in part so that we can gear our presentation toward the group. The votes are still coming in.

This is exciting, watching it change second by second. Well, it looks like the majority, about 60 percent, have a more basic understanding, and then we have a mix of moderate and extensive after that, so terrific. We're glad nobody's just here because they wanted to watch while they ate lunch.

Ben or David?

Ben Hawksworth: Thanks, Monica. This is Ben. As the exit from the Gartner survey on the left of this slide shows, companies that haven't prepared and planned for e-discovery are likely to spend a lot more in the event they're faced with litigation requiring the discovery of electronic information. That's not surprising, given that many companies that incur high discovery costs have not considered beforehand how they might reduce those costs while still meeting their discovery obligations and made plans to that end.

Companies that haven't addressed this issue and established such a plan are very likely to over-preserve and incur greater costs or under-preserve and risk sanctions. The excerpts on the right paint a mixed picture about the preparedness of companies. On the one hand, more than half have not identified 30B6 witnesses who can testify about electronically stored information in the custody and control of the company.

On the other hand, an AIIM survey showed that nearly 70 percent are prepared, with a formal system to manage preservation and legal costs established. In practice, we find that many companies' definition of a formal system for preservation and legal holds can vary significantly.

In some cases, a written policy and guidelines may be considered sufficient, while in others the company may have established a comprehensive plan around e-discovery. In part, this may stem from the legal and discovery risk a company perceives that it has, either because of its litigation history and its environment or the level of regulation that it's subject to. And it may also result if the company has yet to focus on and think through that risk, the impact it may have and the level of preparedness appropriate to the risk.

In our view, the level of planning and preparedness is appropriately tied to the legal risk, yet the company should still consider the people, process and technology components of a well-designed discovery response plan and make a focused determination around the level of planning and capability that it ought to have in place to mitigate its risk.

Monica?

Monica Palko: Great. So one of the biggest questions is, when do I have to start preserving documents? Certainly, we know we need to when we receive a subpoena or when we're served with a lawsuit, and there are some other fairly bright lines – for example, when there's a regulatory obligation or an agency rule. But what about the duty to preserve when a company reasonably anticipates litigation? What does that mean? Because threats of litigation obviously come in a variety of forms, and most companies can't afford to be whipsawed about over preserving documents because they're hearing rumors about any spurious claim. And yet even media reports or demand letters can actually trigger a preservation obligation.

And, what's worse is when a company reasonably anticipates litigation can actually vary in different jurisdictions. Most of us are familiar with the Zubulake case where the court ruled that the duty to preserve actually arose five months in advance of an EEOC charge, and that's because the company was aware of e-mails of various other employees which indicated that the employee planned to sue.

But then we have the Land O'Lakes case in which there was a demand letter claiming possible trademark infringement, and the court ruled that did not trigger a duty to preserve because it discussed a non-litigious resolution of the dispute. So, unfortunately, determining the preservation start point is not always easy. Now, frankly, many companies have also experienced that determining the preservation endpoint can be just as difficult.

What if you're preserving in advance and the lawsuit never strikes? When are you clear? Now, taking a conservative approach may have cost repercussions, but it least it won't lead to some other types of issues that can actually be of much greater concern to the company, and we're familiar with these. A spoliation or an adverse inference instruction, which is to say that a presumption against the company as to what that document that has been destroyed would have said and a presumption that it would have been negative.

In an investigation, there can actually be obstruction of justice charges for destroying documents, certainly monetary sanctions, adverse judgments and these types of things. And even if one manages to avoid those ramifications, you're certainly dealing with a loss of trust and credibility with the other side.

David Wetmore: Thanks, Monica. This is David Wetmore. Looking at how we see companies building discovery response programs and trying to respond to the issues that Monica has outlined, we have a point of view that kind of highlights several different aspects here.

First and foremost, developing the framework is relatively easy. There are going to be variations in terms of the strategy, policy, plans and methodologies that each organization will develop that are unique to that organization and some of the variations are going to get into aspects of how detailed, for instance, policies and plans may be, how much flexibility there is in methodologies to reflect proportional responses for different kinds of litigation, to reflect the particular industry factors, particular company factors related to the historic litigation portfolio that the company has had.

But, overall, looking at this from a high level, the framework is easy to develop. The key, really, in doing this successfully, having an effective discovery and response program is in the implementation, how you take those policies, those procedures, the documented methodologies, and make them active or make them vital so that they can be followed consistently when the fact basis warrants an consistent treatment. One of the things that's critical to think about here is how governance plays into keeping the program vital, how governance can assist in managing compliance, and how through an effective stakeholder involvement process, that includes legal, IT, a risk-management function, to the extent your organization has one of those, how the stakeholder involvement can assist with an evolving, continuous improvement process. So that the discovery response program you put in initially, as a version one, and you continue to execute on that and enhance it over time.

Next slide. Our second polling question, has your company established a discovery response program? And it looks like the majority of our answers are going to be in our program is under development and we don't have a program, which is a little bit in conflict with the AIIM survey that we saw early on in the presentation that Ben talked about, where over two-thirds of companies report having a program in place.

Monica Palko: I think our anonymous polling is much more effective.

David Wetmore: I think that's probably true.

Ben Hawksworth: So why are response teams necessary? The response teams are an integral part of the discovery response program. They participate in designing and building the program and they'll also be called on to implement and support the discovery effort in the event of litigation. Response teams and discovery response programs are increasingly important because of the expectations that both civil courts and the government regulators have regarding the level of capabilities the companies have, or ought to have, to respond effectively and efficiently to a discovery requirement.

That means that both the courts and regulators expect that companies know where their records are, whether those records are likely to be relevant to the litigation or the investigation, how to preserve them and how to produce them timely. In our experience, that frequently isn't the case. In practice, information technology systems generally don't incorporate functionality that supports discovery and information technology departments generally aren't designed to efficiently undertake the discovery process.

Rather, both the systems and the organization are designed to support the business goals of the company. Often an IT organization may not even be fully aware of all the systems that it has that actually contain data or may have set piles of data tapes but little or no idea what data is actually on those tapes. This isn't the reality, though, that either the courts or the regulators are particularly sympathetic to.

Of course, the regulators also increasingly expect that companies will be able to produce electronic information more quickly, simply by virtue of the fact that it is electronic information. Ironically, though, many companies have developed strong records management capabilities around paper records but have relatively less capability around electronic information, meaning that the company may actually find it more difficult to understand what electronic information it has than would be the case if the request was for paper. Here again, of course, the regulators expect the have rational and effective procedures in place, where many have yet to establish such procedures.

If a company is to develop an effective discovery response plan considering all these expectations and the ability of the company to meet them, then a discovery response team that can look across tradition corporate boundaries between IT, legal, records and other units that may traditionally be soloed, and that becomes essential to the success of the program.

Next slide, please.

Monica Palko: So what are some of the advantages to having a response team prepared in advance? Given the circumstances and taking into account the totality of the severe ramifications of document destruction, combined with the fact that exactly when to begin preserving is not going to be clear in every instance, the best approach is to have a response team prepared in advance and a plan in advance so that the decisions can be justified and, as David and Ben were just discussing, if you make a rational decision and you can justify it, you may fare much better down the road.

Also, to be clear, the team doesn't have to be extensive and it should be geared toward the needs of a specific litigation. Perhaps for a smaller case, an in-house attorney and paralegal might be a sufficient response team. But in another matter, maybe a much larger team is needed. Possibly they'll need to span global offices, and that may be important for larger or more complex investigations or lawsuits.

But there will always be an advantage to having the team is prepared with documentation of its actions. Yet again, it should be appropriate to the litigation. E-mails going from the paralegal to knowledgeable employees may be sufficient in one case. In another case, you might actually want your outside counsel to be documenting the measures that have been taken. The bottom line is if you prepare in advance to be second-guessed later, you're likely to make better decisions and you're likely to have documentation of those decisions if it's needed.

David Wetmore: This is an example of a governance framework for a discovery response team, and the slide is a little bit difficult to read. On the left slope of this pyramid is a data governance board, and at the top you see the discovery response program. Beneath that, we have stakeholder groups, legal department, IT, compliance, et cetera, and then we have the functions that a discovery response program will typically incorporate or manage, legal holds, document production, identifying data, preserving data, collecting, reviewing and analyzing it, producing. And then below that the typical records management life cycle steps, create, capture, et cetera.

We also have ESI sources in this data governance framework, and then below that you see the records and information management program that manages all the ESI within the org. The point of having the governance framework here is not to put this forth as a prescriptive model that we believe every organization needs to follow, but really to offer it as one example of a data governance framework for a discovery response program.

The prescription that we would have here is organizations should have a governance framework for their discovery response program. The way that it's implemented at an individual organization will vary, based upon many factors, size of the organization, compliance and risk management functions the organization may have, culture, industry and so forth. But the overriding message for us is the effective discovery response program is a critical aspect – a critical aspect of that is having the governance framework here.

The way that an organization builds a governance program and the makeup of a data governance board is going to vary based upon the company's circumstances and the company culture. Another thing to look at when you're looking at designing a governance program for your organization is to look at the functions in the discovery response program and determine the role that each stakeholder would have in managing the policies and procedures related to those functions.

So, for example, within your organization who's responsible for responsible for preserving the ESI once it is identified? Who's accountable for that preservation being accomplished? When you're looking at identifying sources of ESI within scope of a particular matter, who is responsible for identifying the sources that fit a particular description that legal may have developed?

An important thing to bear in mind is with a government organization only one stakeholder can be accountable. One stakeholder will be accountable. You may have a different stakeholder responsible for execution or for approvals. Others would be consulted and others would be informed, but there's only one that can be accountable.

Next slide.

Ben Hawksworth: The roles that I'll talk about here are those that we would typically expect to see, but the actual roles are going to depend on some of the factors that David outlined in his previous slide, discussing governance.

Response teams will draw from the corporate departments that have a role in discovery. They may also include personnel from business units where the business unit is considered to have a high risk of litigation or is in a highly regulated business area.

The General Counsel's office, or the legal department, will play a leading role both in discovery response planning and in the execution of the plan in the event of litigation or a regulatory inquiry or investigation.

Team members from legal will develop plans to determine the scope of the matter, issue and monitor legal hold notices, assist in identifying the electronic information that should be subject to preservation, and they will also oversee outside counsel retained by the company to support the matter.

Records management will develop records management policies, retention schedules and other instruments that support an organized approach to the management of electronic information that's potentially subject to a hold and they'll assist in identifying that information subject to the scope determined by legal.

IT supports the cataloging and mapping of electronically stored information, focusing in particular on the information most likely to be subject to discovery and works with records to apply records management policies and schedules to electronic information.

IT will also identify preservation mechanisms for major systems, prepare an approach to the identification of relevant data and plan for the preservation and collection of potentially relevant ESI, should that requirement be triggered.

HR and other departments can contribute a range of information necessary to the whole. Those might include the names and organizational roles of individuals potentially in possession of relevant data. It might also include putting together plans for the tricking and reporting of custodians who might depart the company in the middle of an e-discovery requirement or in the middle of a legal hold to ensure that the hold remains in place for these custodians.

Business unit leaders may have particular knowledge of data repositories and information potentially subject to a hold and so may be included for that reason. And compliance monitors the preparedness, testing and evaluation of the plan.

Program management is a little different. Program management takes on the role of the product management office. They provide organizational tools and processes to manage and oversee a discovery project. Program management may be drawn from the company's project management office or it may be temporarily provided by third-party advisers.

Next slide, please. Another polling question. Have you built a response team in your company? And it looks like most are reporting that they do not have a team and a small number have a cross-functional team, have one or two people participating in the team or have one person who acts in a role similar to an e-discovery liaison, but nearly two-thirds don't have a team, which isn't terribly surprising.

Actually, go ahead, next slide, please. The discovery response program that the response team will implement will be in a state of continuous development as the program is tested by discovery event, refined and tested again, which is something that we've tried to capture in the diagram that's onscreen currently. The discovery response program will influence and be aligned to the records management program. The records management program manages the electronic information that the discovery response program requires, and as such the discovery response program will require adjustments to the records management program.

And the records management program will sustain an increasingly sophisticated discovery response program as it moves through repeated discovery events. A discovery response program supports preparedness for litigation, including the development of data maps, identification of perspective (B6) witnesses, selection of review tools and development of response plan, and it is tested in execution, where the plan enables rapid and effective identification of custodians and relevant data and the implementation of the legal hold.

The records management program dovetails with the discovery response program, establishing the organization and instruments for effective records management, which themselves are then tested by the discovery event, leading again to improved classification of electronically stored information and supporting the updated maps of ESI that themselves support the discovery response program.

So this is a process where discovery response and records management tend to feed each other and depend upon each other and are improved and made more relevant to the process needs of the organization, as discovery events manifest and are dealt with and themselves influence the records management program and the discovery response program.

Next slide, please.

Monica Palko: Great. Now, this slide is deliberately packed with words, because the point of it is that the scope of electronically stored information is truly mind-boggling at this point. Of course, we have the standard paper documents and file drawers that we've always had. Today, those are more likely to be personal copies with handwritten notes and the like, in addition to copies that will be found on people's computers, but people still work in hard copies. We also are going to have the classic sort of voice-mails that used to be just stored on a phone, on a desk, on a company system, not so much anymore. We've got Word files.

But, in addition, there's been this tremendous explosion of ESI. It's instant messaging, it's texts, it's voice-mails that are on additional things like cell phones. You've certainly got your PowerPoint presentations, pictures, Web pages, and in addition there's an obligation to preserve the metadata for all of those types of things. But even more, where are these various types of documents stored?

Now we've got various types of phone machines, as I mentioned, cell phones had the like. You've got your laptops, BlackBerries, Palms, iPhones, other types of handheld devices, hard drives that are going to be on the desktop but they might be freestanding hard drives, CDs and thumb drives that people could be storing their information on.

In addition, if you're a multinational corporation or you have offices in other countries or you might be outsourcing some matters to other countries, it's not unusual now, especially for document review to be taking place in India or other places. And perhaps there are some documents stored there.

You may be dealing with foreign languages, foreign lands and certainly foreign cultures, where the discovery process that might be imposed in the United States may not be easy at all to impose in a foreign country. So think about it. If you had a sudden need to lock down documents, all those types of documents on all those various sources, could your company do it? And even if you could lock it down, would the documentation of those efforts withstand scrutiny?

So, as you might imagine, we have another polling question. What's the greatest document retention challenge facing your company?

Interesting. We need to wait for people to weigh in until we get a true result. I think the anonymity of this is important, too, because employee cooperation, right, can be a really difficult aspect. If you're actually lacking employee cooperation, so that they're walking away with thumb drives and laptops and the like, that could be a real serious problem. Some just don't realize how important the document preservation efforts are and you need to establish sort of a more demanding e-mail or have greater repercussions if they fail to respond.

I actually find that the costs can be quite excessive and that courts don't seem to be very sensitive to that. But it looks like we're coming up with almost equal parts, expect for we aren't seeing, I guess, a lot of cross-border language differences or cultural differences. But these are some of the most important challenges that companies find when trying to implement their document holds.

David Wetmore: So then we look at what tools a discovery response team should use to overcome the challenges that the last poll talked about. And we tried to present this in the most helpful manner we could, so we took the approach of preparing a check list that you can use to assess where your organization is and then for each of the items that we've listed here, if your organization has it, you can do an assessment, a self-assessment, even, of how effectively those tools are working for you the way that they're currently designed and the way that you train on them.

When we look at what it takes for a discovery response program to be effective, these are the basic tools that we expect to see. We do think it's important to have an ESI map that provides that inventory of systems and data that will give system ownership, the methods that you use to preserve data in the system when that's required. Potentially, the ESI map will include historical information related to the system's use, predecessor systems or related systems. So that when you're looking at scope for a particular matter and you refer to the ESI map, you can use that to validate that you're putting the boundaries, preservation boundaries, in the right places for your various systems that are at play for that matter.

A hold tracking tool is going to enable you to document the scope of the preservation for a matter, identify the custodians, individual custodians or IT custodians who are responsible for managing the data that you have in scope and then managing the communication to those individuals or those IT custodians.

And, as Monica said earlier, on some matters a hold tool or a hold management tool may be overkill, where you only have one or two custodians and it would be perfectly effective and perfectly reasonable to follow an approach of a paralegal communicating directly with the custodian through e-mail and managing the communication, correspondence and reporting through that method. So that's one of the things that we would have you look at as a you're putting together a discovery response program is what's your litigation portfolio like historically? What are the kinds of cases that you have the number of custodians involved?

And you would right-size, to use a nice consulting word, the tools that you're going to use and the processes that you're going to use so that they make sense for your environment, for your organization.

For companies that do implement a hold management tool, this can be a very effective way to manage follow up and to manage escalation where there's no record of appropriate action being taken and a hold management tool can also be a very effective way to enable compliance processes within your organization.

Next slide.

Ben Hawksworth: The process that your discovery response team is going to follow is going to follow essentially the outline of a typical legal hold, so if that legal hold is broken down into components, then processes need to be established around each of those components, and those are also similarly represented here in sort of check list format. The process requires a plan to establish the approach to the discovery project or the determination around the scope, including custodians and data sources.

The response team will be activated and, again, this is from a proactive standpoint, so in each of these instances the response team is preparing a plan or an approach to address these items.

So the response team will be activated to implement the plan. They'll form a steering committee or some similar organization to guide implementation of the plan and decision making around data preservation activities. Custodians will be notified of their preservation obligations through a preservation notice with sufficient detail to enable them to meet their obligation. ESI within scope will be identified and preservation activities will commence, including preservation of data on business systems, not necessarily in the actual custody and control of the individual custodians.

Existing holds will be cross-referenced so that a determination can be made regarding the risk that data released from another hold that is relevant to the current litigation might be destroyed. And compliance by individual and business system custodians will be monitored and tested to ensure compliance with the process.

The legal hold is documented to increase the defensibility of the hold should it become subject to scrutiny and exceptions, such as lower-than-expected counts of e-mail or documents are investigated and reported on. Lastly, the team should be prepared for the lifting of the hold and subsequent distribution of data, as long as the data does not cross-reference to another hold. So obviously in this case we're trying to account for the possibility that holds overlap.

Next slide, please.

David Wetmore: So as you're putting together a discovery response program and looking at some of the items that Ben and I have just described, what are the sorts of risks that you should be considering?

What you see here in this initial summary of risks really underscores that the root cause of many discovery problems or discovery challenges is insufficient or inadequate records and information management. So one of the situations that we quite commonly see when we assist clients with discovery is that there is a lack of developed records retention schedules, leading to a dramatic over-retention of records within the organization.

So the collection of data, the sweep for potentially responsive ESI yields a much higher volume of data than it would if the company followed retention schedules and followed good records management, records and information management practices.

We also see, in a related root cause, that companies typically have inadequate records management infrastructure and policies. So what we see as successful strategies to help mitigate those risks is for the organization to look strategically across its enterprise for records management issues, develop a uniform approach for records management and a uniform approach certainly can include business line or business unit variation as applicable for the specific business.

Typically, a uniform approach would establish a minimum standard or a set of guidelines that individual business units would follow and then business units can go to greater granularity of detail or a more stringent standard of training or compliance, et cetera, than the overall organization requires.

We also think that for organizations to really make any progress with effective records management infrastructure, they have to be prioritizing based upon business risks that the organization faces. So our first bullet under strategy, prioritize business lines with high discovery risk, is certainly a very effective way to help mitigate issues related to inadequate or ineffective records and information management.

Probably the key takeaway from this slide, or this concept, is that as you're making investments in strategic and even in tactical discovery response efforts, it's very important to include a risk management framework as you're creating your plans and then executing on the plans.

Next slide.

Ben Hawksworth: These are some of the technology risks that we see response teams encounter as they try to develop a discovery response program, as well as some of the strategies for mitigation of those risks that we've seen be successful. And, of course, these aren't all the technology risks, but they highlight some of those that may be prevalent.

Inconsistent responses to discovery requests pose the risk that a position taken in one method might be contradicted by a subsequent position on a different matter. Developing standard responses to discovery requests can mitigate that risk, as long as they're kept up to date and accurate. We do sometimes see binders pulled out with responses that date back to 1995. It's important to make sure that they're kept up to date.

The lack of an adequate inventory and electronic information could lead to over-preservation or under-preservation, leading to the risk of either increased cost or a greater risk of sanctions. In particular, the distribution of electronic information repositories around the organization increases these risks. It simply makes it harder to determine where the data lives and also how to preserve it and prevent it from being destroyed, and later, to collect it.

Centralization of repositories, such as in a document management system or in an electronic records management system, can reduce that risk, by centralizing data and placing controls around the data so that it doesn't get distributed across the organization in an uncontrolled way.

If a plan for preserving and collecting emerging data sources, such as instant messages, does not exist, then the company will be in the position of evaluating both the risk posed and the approach to dealing with the data source itself actually in the heat of battle. Identifying those sources beforehand supports effective planning and mitigates the risk that if you don't have an awareness of how to actually address that type of data when the issue arises, then you're going to have to figure that out.

And by the time it's actually figured out, you may actually have lost some of the data and be at risk. Many companies maintain obsolete or legacy systems in media, such as backup tapes, that can contain potentially relevant data or might contain and oftentimes they have no idea what's on it, but there's some risk that relevant data might be on it. Evaluating the challenge of preserving and collecting data from these systems and those media can prevent a fire drill and mitigate significant risk if it's done ahead of time and formally, as part of a discovery response plan.

Next slide, please.

Ben Hawksworth: No discovery response program is likely to be consistently implemented if compliance is not a core component of the plan. For one thing, having a compliance element to the plan demonstrates that the discovery response program and the response team's role is a serious one and it's not simply a showpiece that's being done for the benefit of the courts or the public.

Periodic evaluation, review and testing of the discovery response program and assessment by the response team is important if the response team is going to be able to gauge and demonstrate compliance with the program. So here we say that employees will do what you inspect, and not what you expect, which is just a shorthand way of saying that the plan is not likely to be implemented in a consist and effective way if somebody's not watching and testing and making sure that that's done. And that is a critical role of the response team, to monitor compliance with the program itself, to stay on top of it and to help guide the participants in the plan to deliver effectively within the parameters of the plan.

David Wetmore: One of the things that we're engaged with clients to assist with on a fairly regular basis really is narrowly that compliance aspect of their discovery response. So in the case-specific work that we do, it's quite often the case that the client has identified as a very targeted need and a specific area of focus for us to assist them with both performing the case-specific compliance efforts that their program calls for and helping to make sure that the documentation for those efforts is adequate and will withstand challenges, should any challenges arise.

Monica Palko: Great, are we ready for question and answers? We actually have a number of questions. Thank you, bring them on. I'm going to combine a couple of them. We certainly talked about proportionality in terms of what the litigation or regulatory requirement would be in terms of the response team needed and how that would be documented. But we have a couple of questions related to the size of the company.

What if we're at a company that's only 100 employees total? What if we're at a company where we have a team of six managers and then basically administrative personnel below? How extensive should the program be?

Ben Hawksworth: I think the discovery response program is typically going to be tailored in two ways. First, it's going to be tailored to the needs of the organization, and that means what level of litigation history has the company had? How extensive is its litigation portfolio? And in a smaller company, that's typically going to be less than in a larger company, many of which have a constant and ongoing number of litigation cases that they're handling.

It also needs t be tailored according t the regulatory environment that the company operates in, so if it is subject to significant regulatory scrutiny, then it's more likely that there will need to be a more comprehensive effort to build both a discovery response program and a discovery response team to support it and to execute on it in the event that at discovery requirement surfaces.

But in a smaller company, that plan and that team is likely to be bound to the needs of the company, taking into consideration just what that litigation portfolio and the regulatory environment looks like for the company. So from an organizational standpoint, the first task is to make sure that it's balanced to the needs of the company, and typically a smaller company is not going to have as much litigation nor be subject to quite as much regulatory scrutiny.

The second is the nature of the matters themselves. If it's a small matter, if it's a slip-and-fall matter, versus, say, a significant investigation, then the level of effort that's put into discovery is likely to be tailored to the – or should be tailored to the needs of the matter. You're just not going to put quite as much effort into responding to the discovery requirements of a slip-and-fall as you would into a large investigation.

So, again, it's important to tailor the discovery effort to the needs of the matter. Now, if there are matters that are of like size and need, then it's going to be extremely important to make sure that they're all dealt with in the same way, that the preservation planning and execution is similar for each of those matters because you don't want to get into a position where you effectively are more diligent in your discovery around one matter than you are around another.

Monica Palko: David, anything to add?

David Wetmore: No, I think that's a good answer.

Monica Palko: We have sort of an offshoot of the question, which is for a small company, can't the IT company simply confirm that the IT provider can do a system save and do a disk drive of some sort for the litigation. So I think the point is that if you're able to identify a group of documents that was developed in the past and it's not ongoing and continue to build day and day, regarding an ongoing project, you probably can lock down those documents, whether you put them on a disk or whether you hold them on a server or a backup tape.

But I think the tougher question is when a project is ongoing, so there may be litigation regarding an ongoing project and you continue to develop documents day to day. So I certainly think in an ideal situation you would be able to have a third-party provider simply lock down all existing documents and not have to worry so much about the ones that are continuing to be developed.

David Wetmore: And with that question, Monica, I think it's important to note that if you're using a third party IT provider, even for a smaller organization, it makes sense to in advance work through with them and have as part of your agreement with them the method or methods they would use at your direction to preserve data, both in a historical situation and in the more complex situation that you describe, where you have an ongoing requirement to preserve.

Monica Palko: Right. And this raises a good point and another question that was coming up, which is when is it better to use a third party to harvest your ESI, versus go ahead and do it in house. At BearingPoint and similar companies, we're actually pretty fortunate because we have technology-savvy individuals and we're able to give them instructions that they readily understand and can follow, which makes it a little easier. But third-party providers actually also have advantages.

What David was just saying is really important. A third-party provider should have defensible procedures that they have in place and they know how to harvest the data without altering that metadata. And folks with smaller IT departments may really not have that capability in house, and you can destroy metadata if you don't harvest the ESI properly.

And, what's more, a third party can actually provide independent testimony if that's ever needed. So if there's going to be a 30B6 witness, if you need a testimony of an individual as to what procedures were taken, you certainly don't want your in-house counsel having to sit on the stand and answer questions about that. You're going to have privilege issues.

But if you have a third-party provider who handled it, then they can go ahead and be the ones who provide that independent testimony, which can be a really good thing.

Ben Hawksworth: Monica, I'd also add to that, oftentimes, in a preservation environment, you really have one opportunity to get it right. And sometimes what happens is a laptop, for example, needs to be preserved, or rather the data on the hard drive needs to be preserved and it'll be preserved using a tool that, for example, doesn't capture deleted data on the disk.

Now, that's not always going to be necessary. But when it is, if it's not done correctly, then that laptop is returned and essentially any further work done on that laptop might then destroy that data.

When it comes time to look at what was done, if you find out that in fact the wrong tool was used, it was not configured properly, then that opportunity may be lost and that may create a very significant and difficult challenge for the folks who need to make some statement about what was done and how defensibly it was done.

Monica Palko: Great. Here's one. They all just seem to be rolling in a related way, but the question is, do you recommend that the legal department collect all documents covered by a legal hold prior to litigation or wait to collect the documents after litigation has commenced? This is one where I would say ask your outside counsel what's appropriate in any given case, but what can happen is if you're preserving because you reasonably anticipate litigation, because you don't have to produce them, or what often happens is you receive a dramatically over-broad subpoena and even the propounder of the subpoena does not want a massive data dump, so you agree to actually produce a smaller subset of documents.

Sometimes it can be so expensive to go ahead and collect up the documents – where do you keep them? Where do you store them? Just as Ben and David were discussing, you can have metadata issues associated with moving them. So I think many companies choose to look down the document and preserve them, as long as they're comfortable that that can be done, without actually physically gathering them and moving them if they don't actually have to be produced. But I certainly welcome Ben and David's thoughts on that.

David Wetmore: I think that's right, Monica. It's not necessary in every instance to collect the full set of documents that you're preserving. There are clearly distinctive sets and there's essentially a process flow handoff between preservation and then collection and then even a further handoff to review. So think of it as a funnel and you're preserving more data than you're collecting, and you more than likely are collecting more data than you're reviewing because you're going to have filters and de-duplication and so forth that allow you to further reduce the set of data by the time you get to review it.

Ben Hawksworth: One case where you might end up collecting at the same time that you preserve, as it were, is in the case of, say, a fraud, where you simply need to collect it, you can't afford to leave it in place where it might be altered, and so you just need to move forward with collection and you collect everything.

Monica Palko: Right. All right, we have about five more minutes. Here's a good one. Where does a discovery response team typically report?

Ben Hawksworth: We frequently see an informal reporting structure, where there is not really a reporting – a top-level report, as it were. But to the extent that it happens, it's typically into the General Counsel's office, or into the compliance office, which itself might be a part of the General Counsel's office or it might be part of a separate organization. But where there is a report, those are typically where the report is.

Monica Palko: And I find as well that what's appropriate in any given situation may differ. If the compliance team is conducting an investigation, it may make sense to have everyone report into someone at the compliance team, whereas if you have someone in litigation who's handling the litigation, it might make sense to have that individual essentially leading the team.

And then I think you're going to have different subsets. For example, someone in litigation might report to the General Counsel, but if you have someone who's in the IT department or in a records management department, they might report to the head of IT in addition, or they might report to the head of a global real estate or a shared services group that handles the general records management decisions.

So I think you're probably going to have to decide in any given instance who takes the lead.

David Wetmore: I think that that's right on a case-by-case basis. And one of the things to bear in mind, any time you have a cross-functional team or a multidisciplinary team in an organization, is there are going to be multiple reporting lines. So an IT representative on a discovery response team is going to have their IT manager that they report to, and they're also going to be reporting as a discovery response person into the data governance board, whether that ultimately reports to the General Counsel or the Chief of Information Security or compliance, depending upon the organization.

So there are at least two different things going on when we talk about reporting. One is how the program and the people in the program report up, and ultimately that means who's accountable at the governance level. Is that a triad of Deputy General Counsel, IT organization and compliance or risk organization? It may be in a large organization that it's structured that way. But then, moving beyond that, as Monica just said, on an individual matter basis, who does the execution team report to? Is it a litigating attorney who's responsible? Is it somebody in compliance who's meeting an internal investigation, or exactly where does that execution team report?

And the governance program and project execution are different but related, and that's just something to keep in mind as you're looking at how simply you can structure a discovery response program and where you're going to have complexities.

Monica Palko: Great. Well, I see the we do have some additional questions, but I want to be respectful of everyone's time. So just as a reminder, you can complete the webcast evaluation form and ask your questions there and we will receive your question and Ernst & Young receive the question and we can follow up. Also, as a reminder, regardless of whether you have a question, please complete the webcast evaluation form, and we refer you to the info pack and you can get there in the links box on the left side of your screen. There was also a logistical question, someone who was interested in printing the presentation slides.

Just so everyone's aware, you can click on them here and print them. And also the webcasts are archived, so you'll be able to go into this later. If you have any questions or issues about that, here is our contact information, and you can certainly e-mail any of us directly and we'll make sure that you receive the presentation slides.

And the info pack also will e stored in the group of info packs in the ACC learning site, so you'll always be able to access that separately, as well. So I think we have to close, but we thank everyone for their active participation. I want to especially thank Ben and David, and that will conclude the webcast.

Ben Hawksworth: Thank you, Monica.

David Wetmore: Thanks.

END