ASSOCIATION OF CORPORATE COUNSEL

TITLE: **Security Issues in Complex Outsourcing Transactions**

DATE: **November 13, 2008**

PRESENTED BY: **ACC IT, Privacy & e Commerce Committee**

SPONSORED BY: **Hunton & Williams, LLP**

FACULTY: **Jon Bancone**, Associate General Counsel, IBM Technology Services
Orrie Dinstein, Chief Privacy Leader and Senior Counsel – IT & IP, GE Commercial Finance

MODERATOR: **Jim Havey,** Partner and Co-Chair, Global Technology Outsourcing and Privacy Group, Hunton & Williams, LLP

*****

Operator: Just a reminder, today's conference is being recorded. Welcome to this ACC webcast. (Jim), please go ahead.

(Jim Harvey): Thanks very much, (Kelly). This is (Jim Harvey). I'm the moderator for the conference today. And, I'd like to thank everyone for joining us for what we hope will be a very valuable session. And, I'd also like to thank the ACC, the Association of Corporate Counsel, and, in particular, the committee, the IT E-Commerce and Privacy Committee that is sponsoring this. We hope you are all members of that committee, and will participate in a number of great activities we've got planned throughout the year.

For the participants on the call, you can participate by the chat function at the lower left hand side of your screen. It should be pretty obvious how to send us a message. Send us a message at any time that you'd like during the presentation, and we will either respond to it right then or put it at the end if we can get to them all, et cetera. We may not be able to respond to all of the messages, but we will attempt to do so. So if you have questions, I would encourage you to hold those questions until the end because we think this is a holistic topic. So, maybe, jot them down, but if it's something that you think needs to be brought up right then, by all means, put it in and we'll see if we can get to it.

So, that being said, I want to welcome my co-presenters, today. First off, we have (Orrie Dinstein) who is with GE Commercial Finance. (Orrie) is a thought leader in this area and in technology and privacy and security law in general. He's the Chief Privacy Leader and Senior Counsel for Information Technology and IP at GE Commercial Finance. (Orrie's) responsibilities include data protection, technology licensing, computer security, e-commerce and intellectual property matters. So, (Orrie) has a very, very wide plate, but it is one that I think lends itself particularly well to today's conversation.

We're also joined by (Jon Bancone) who is with IBM. (Jon) is Associate General Counsel of IBM. He is currently assigned to Global Technology Services in the Americas. He provides and oversees legal support for the sale and delivery of outsourcing, hosting and maintenance services in the U.S., Canada and Latin America.

(Jon) and (Orrie) and I have given this presentation before, and I'd also like to say that I've negotiated on the other side. I mostly represent customers. I've negotiated on the other side from (Jon) and we often disagree about things. But I've found (Jon) and (Orrie) to be thoughtful and insightful with respect to this topic, so we're glad to have both of them today.

My name is (Jim Harvey). I'm a partner and co-chair of the Global Technology Outsourcing and Privacy Group with Hunton & Williams, and I'm in the Atlanta office.

We've got a couple poll questions – actually three poll questions, today. You can see on this slide if you just click to the left of your screen, you will – to the left of the list there – you will be able to let us know who you are. We've just got a couple – we've just got a couple, sort of, demographic slides, if you will, that will let us know who we're dealing with, what the proportions are, et cetera.

The first question is what best describes the industry in which you work. Self-explanatory – technology, manufacturing, financial services, et cetera. Most of the folks on this call are in the technology arena. A few financial services, a few retail, one energy, and others.

The next question is how large is your company. I know these are large numbers for some and small numbers for others. Are you less than $1 billion, $1 billion to $5 billion in market cap, or more than $5 billion?

Given the state of the volatility in the stock market, I'd just say take your best shot at this. Let's do an average across the last year or so because I know people's stock prices are varying widely. It does look like most people are, on this screen, are larger than five billion, which is an interesting demographic. So, more large companies are participating on this phone call. We'll adjust our comments accordingly.

Is your practice primarily devoted to security and privacy matters, or does it include significant other practice activities? So, given that the ACC in-house counsel – sometimes you find people that are very, very dedicated to one topic area.

Generally, I would expect – and the answers are bearing this out – most of the people on this call have security and privacy and other areas. I imagine there are a smattering or tech folks, IP folks, privacy and security and probably some jacks-of-all-trade. So, that's good. We've got largely large companies and folks with more on their plate than just privacy and security.

I thought I'd set the table with a few slides here that hearken back to sort of where we've been in the security and privacy arena. And started with the ChoicePoint. Now, as you can see, this is from 2005, and it was the first, what I would call, watershed event that really brought security and identify theft and phishing and all sorts of online scams into the collective public consciousness, if you will.

We've come a long way since then. If you recall, it was like, this was for – in the news every day for a week or two, and then a bunch more in the following months. But if you look at this next slide, this is just from two years later. This is from January of 2007 for the TJX breach. And, this was sort of another watershed event. I think probably because of the number of people that may have been involved in this breach. This article mentions potentially 40 million people involved with their credit card numbers exposed. And, that was just in January of 2007. How quickly time passes. We basically see these breach notices, I'd say, on average, once a week or so, and that – it is really in the public consciousness now.

The next slide really brings all this together in a very cohesive fashion for today's presentation. This is a slide about a data breach in the U.K., so it points out that this is not only a United States phenomenon. It's dated October 10, 2008, so we see that there has been no slowdown, if you will, in the number of breaches.

In fact, it may have even picked up. But, this slide also includes a breach by a third party service provider. In this case, it was EDS. They're by no means the only service provider that has had breaches. But, that is the one that's mentioned in this article.

In our experience, about half of the breaches that occur involve some sort of third-party service provider. And, that is making our issue today really a very, very hot issue, we say, in complex (washing) transactions – probably better put, it's a hot issue in all technology relationships.

When you start with ChoicePoint and then move forward, there are now about 44 states with security breach laws. There are states that are passing laws and regulations that really go beyond security breach into the specifics of how security should be handled – encryption levels, et cetera, et cetera. We've got a couple quotes here for the Massachusetts regulations, which many of you are probably familiar with. They come out January 1, 2009. And then what I've called the Nevada Encryption Law, which was effective last month. So, the laws are really going beyond just breach notification or, at least, these couple have, and we expect to see some more.

The last bullet shows that this isn't, again, only a U.S. issue. New Zealand, Australia, Denmark, several others either have or have a rough equivalent of breach notification laws. But our topic today is not to go into the nuances of these laws and the trends and themes. Our topic is to talk about how you address these issues in sourcing transactions when you're developing a relationship with a third party.

It is, indeed – I think in the transactions that I've done in the last 24 months – probably the last and the most volatile issue to get resolved because everyone realizes that it's important. So, we'll have some other content during the year for the ACC on the specifics of these laws, but, as you're developing your transactions – we broke it down – (Jon) and (Orrie) and I broke it down into really three phases of the data lifecycle in these transactions.

The first phase is really understanding your data environment. I think our high-level takeaway is that this is – there's not a monolithic position for security and sourcing or technology relationships. You need to develop your positions in context.

Generally speaking, the most typical request that I did at the beginning of a transaction is, I want unlimited liability for anything having to do with personal data. And, sometimes that relates to the transaction, sometimes it doesn't. (Orrie) you may have some comments on some of the rest of the drivers on this slide.

(Orrie Dinstein): Absolutely. Thanks, (Jim). I think that one of the biggest mistakes a company can make when it embarks on outsourcing is to simply, I'll say, contact the vendor, whether it's through an (RFP) or through some other reference that they have, and immediately start the process of negotiating the outsourcing contracts, often with a focus on price. That leaves out a lot of crucial analysis that has to happen on the front end, which is – the key issues are listed on this slide, and I'll mention them, but a few others that aren't on this slide.

So, certainly, I would think you want to start understanding what it is that you're outsourcing. If you're outsourcing just a specific function, like HR, if you're outsourcing a specific service, primarily IT types of service, or if you're engaged in BPO, which is business process outsourcing, and each of these have different characteristics and will involve very different types of issues and concerns.

And then you, obviously, have to consider what are the drivers for the transaction. Is this primarily about reducing cost? Is this about potentially diversifying your risk by pushing some of it offshore? Does this have to do with a service model and what some people call follow the sun, where you want – if you're a multinational and operate across the globe, you can't have all of your IT support, for example, located in just one place. So, you might outsource it to different countries and different continents to get that continuity. So, there can be very, very different drivers.

And then, of course, you have to take into account what type of data is at issue. Is this personal employee data with social security numbers and salaries? Or, is this potentially you're just outsourcing your helpdesk? Or, are you outsourcing a business process perhaps where someone is reviewing documentation for you to make sure that all the loan documentation is complete? So, it might be a somewhat simple process, which doesn't involve a lot of moving parts.

And then, of course, where is the data coming from? Are you sending all of your data from the U.S., and where is it going? Is it all going to India? Are you outsourcing data from the European Union to other countries, and so on?

And then last but not least, of course, whether or not you're regulated because, to the extent that you have to meet certain regulatory obligations – mostly financial services – I didn't see anyone from the health-care industry, but certainly HIPAA would impose some security obligations on you.

That, again, you would have to factor into the initial assessment. And, all of these things together will come up with sort of a picture of what you can and can't do, what your expectations are, what your absolutely – the must-haves are, what are the things that you're flexible on.

So, if the vendor says, for instance – I can't really service you from India with that type of service that you want, but we've got some great developers in China who can do that work – for some work that might be great, and for other work, that might be a really risky decision. So, all of this has to happen on the front end before you ever contact a vendor and start discussing data privacy and data security types of issues.

(Jim Harvey): I think that's good counsel, (Orrie). The color that I would add to that – and (Jon) may also have some color – but, (Orrie's) comments couldn't be any more on point or precise, if you will, with respect to this issue.

If you are coming in and saying – It's our company policy that we'll get unlimited liability for anything having to do with personal data in any type of transaction, I don't think the market – the market won't respond well to that. Service providers are very, very focused on this issue. I think they see it as one, sometimes, that they can control to some extent and, sometimes, that they can't. And the law is moving so quickly that, if you're going to come at this from the – we're the 40,000 pound gorilla in the room, and we'll get our way, generally speaking, in a negotiated transaction, you're going to encounter some pushback. So, (Orrie) is absolutely right. You've got to make these decisions in context and out of the box.

I also encounter – on this next slide – I encounter, (Orrie), a number of different ways that customers and suppliers deal with this security issue, depending on whether I'm dealing with a regulated entity or a non-regulated entity.

Given that our audience today is inside counsel, I thought it would be helpful if we spent just a little time talking about the structure of security teams and the security thinkers, if you will, that come together in these transactions. I see it all over the map. Sometimes there's a chief security officer. Sometimes there is a sort of a third party assessment team, and you get programmers and very techie types who can't make a holistic analysis of the situation.

I wonder if you'd give us a few comments on – your thoughts on who are involved and when and how they get involved in the security portion of these transactions, (Orrie).

(Orrie Dinstein): Yes, and, obviously, this is my own perspective from how I see things happening at our company. I can imagine that other large companies might operate similarly but not always. And smaller companies would operate totally differently because you probably would have far fewer people and people wearing multiple hats.

The business decisions, of course, are typically made by the business team and sourcing, and that's where you would get into the, kind of, initial review. Are we doing BPO? What country are we going to? How many vendors do we want to consider? Price, of course, is a main issue. Reputation of the vendors? Do we have any past experience with them? Why are we looking to do this – so, again, one of the business drivers.

All of that typically gets fleshed out by the business together with the sourcing team and the function that's involved. So, if you're outsourcing HR, HR, of course, will have a key say in that discussion.

Once all of that gets baked down and we engage a vendor, that's when our legal team typically gets called in to start negotiating the contract. And, of course, we – I'll focus on the privacy and security aspects. As the privacy leader, I tend to bear the brunt of the negotiations for those clauses.

And while I will consult with our security team, I don't bring them to the table on the front end. I find that, at least initially, it's more helpful to understand what the issues are, where the vendor is pushing back on our requirements or on our policies, and where the vendor is, perhaps, saying – I can do things this way, but not that way. And that's when I'll probably go and get the security people in and say – well, they can't encrypt our data, but they said that instead of it they'd do something else. Is that something else, in your mind, sufficient?" Those kinds of conversations.

So, security, in my mind, is more of a consultant to the team or a – if there's not a team, to the person who is negotiating the contract and not in the driver's seat.

(Jon Bancone): (Orrie), on the vendor's side, I mean, we recommend that the vendor security teams engage early on with the customer security team not only – not only during the due diligence phase but also, obviously, the solution design phase. One of the issues is that you need to be able to understand where certain data sits in order to design a system around it.

So, for example, if you have a system that's – that has PII on it, you may want to have different security around that environment than somewhere else. So, we feel strongly that the security teams of both sides should get heavily involved.

Now, obviously, if you're dealing with a small company that doesn't have an independent security team, there is a decision maker at the customer level, on you know how robust the security needs to be, and that would be the person engaged at that time.

Having a complete understanding of the environment, obviously, facilitates solution design. And it also facilitates the discussion on puts and takes in connection with the decisions regarding security – the discussion that needs to start before the legal team gets to the negotiating table.

Because once you understand the choices that the customers made, it facilitates the legal discussion. So if a customer chose, for example, to take risk in a particular area, that will facilitate some of the legal discussions in talking about who bears which risks. And, then, as I mentioned, the — you know PII is a good example of that. You would typically design a little bit more robust security around a system that contains PII. By PII, I mean Personally Identifiable Information. And, in that regard, the legal discussion – you know the vendor would have more flexibility in terms of liability that we'd be willing to take on if, in fact you know a more robust solution is offered up and accepted by the customer.

(Jim Harvey): And, we're going to come back to that point, (Jon), about what service providers take on and how they analyze it, et cetera. But, I do think that the appropriate take away from this – from this slide is early involvement. Again, these decisions need to be made in context because – I think (Jon) will say that – providers are willing to take on a lot more liability in the security space, but that may very well directly relate to what it is the customer is willing to pay for.

So, in (Orrie's) example about encryption – well, they can't do encryption but they can do this. Is that good enough? There's going to be a pricing impact if you go ahead and insist on encryption despite the fact that the service provider says – oh, that doesn't really work or you know it's going to be unreasonably expensive to do that. But, get your teams involved early and be sure that they understand what's going on.

Now we get down to what I consider the fun stuff from a legal and from a contractual negotiations perspective. We think that phase two of this – so, if the first phase as understanding your data in the context of the environment in which you're operating from a data perspective, the second phase in these transactions is defining the service providers' responsibilities.

And, when I sit down with customers, the first thing I say is – do you have a security policy that you are going to impose on the service provider, or that you're going to make part and parcel of this transaction? (Orrie), you may have some thoughts about the way you handle this internally or the way you've seen others handle it.

(Orrie Dinstein): Yes. And, as you can imagine, in a large company, we will have quite a few policies in various security related areas as well as privacy related areas. And, we typically will include these policies in the RFP, and they will be part of a front-end list of expectations of the vendor in terms of what it is that we want or what it is that the vendor needs to meet.

And, if they're not going to meet that, then we need to understand whether it's something that is not needed, or is something that's needed but the vendor can't meet because of cost, or because of something that the vendor has a different solution that can get us to the same endpoint but through a different set of means.

And, of course, there are also external standards, and some of them are listed here. And, I would say that, as a small company, or as a company that doesn't have a robust set of policies, I would certainly fall back on these standards because the one thing you want is a clear set of rules that the vendor has to live by. You can make them up. You can rely on a standard, which is obviously a lot easier, and just say – you will meet ISO17799, or you will comply with PCIDSS, which are the credit card industry data security standards.

But, if you have your own fairly robust security policy, which spells out in great detail what it is that you expect in terms of third party connectivity to your network – handling of personal data, encryption of data, password on devices, physical and logical separation of data on your servers, anti-virus systems, firewalls, physical security, dogs, guards, everything else, then you might say – "I don't need to fall on that standard because, frankly, I think that my policy is just as good as that standard, and certainly it's good enough for me." And, again, that's where you might fall on that.

So, I think that I would hesitate to do both. I would hesitate to throw on the vendor a 50-page security policy and say – "oh, and by the way, also meet the ISO standard," because (Jon) will turn to me and say – "well, what does that add to your policy?" And if I don't have an answer, then I might as well just not tell him to meet ISO.

So, to me, obviously, having a good set of policies is a great way to start. And it's not just the security policies, it's the privacy policies. So, if you have rules for employee data, then, again, you can put them in front of the vendor and say – "we have promised our employees and it's our internal practice that employee personal data will be handled in a certain manner, and this is it. And, this is what you're going to have to live by."

(Jim Harvey): Go ahead, (Jon).

(Jon Bancone): I'm sorry. Just the perspective is that (Orrie) and I are in kind of – our own agreement on this one – I mean you know we want the obligations to be spelled out in great detail because, in large part, too – because you know only really the customer knows what's adequate for their business. We you know – vendors service a lot of different customers in the same industry. And there are players in each of these industries that can vary greatly as to how they handle security.

So, there are completely different approaches even within the same industry. And, they're really – it's a risk tolerance question on the customer side as to what kind of security you want, what kind of performance you want from your systems, and that's a balancing test that every customer is kind of different.

So, there will be trade offs, as (Orrie) said, and the real point that we would have you know as a vendor, is that the only thing we don't like in this area is vague obligations. To say that you'll implement appropriate security, for example, you know doesn't really help us very much because appropriate is customer dependent. And so, we don't really have an answer as to what's appropriate. I just need to know what it is I need to do. And, again, really this whole thing is really a sliding scale – the more specific you are in the obligations, the easier it is to have the liability discussion.

And, external standards are the same thing. I mean we – an external standard is fine as long as it's crisp. So, if the external standard is you know implement appropriate security, well, that's not a very helpful external standard. If you have an external standard, we can take that standard, we can give it to our security team and say – go do the following, and they'll go do that and they'll price that into the bid.

(Jim Harvey): Yes, this is (Jim). Let me – let me see if I can also talk about the rest of the story, if you will. I think in both IBM and GE, we're probably seeing two players who are at the absolute top of their games with respect to security and privacy, both in obtaining it for GE and then providing it for IBM customers.

With respect to this first bullet, are there any applicable customer security policies, you don't have to get very far out of the highly regulated industries until the response to that question will quite frequently become – well, we have them in draft form or we have them but they haven't been updated in two years, or we don't have them at all, or so and so has one for their department and thus and so has one for theirs."

And so, then when you get into the real world of doing these transactions, again, below GE and IBM, you're – the customer is often left with a difficult decision of – well, my policies aren't that good and I know it," or they don't exist and I know it. So what do I do?

A lot of times, customers will, I think, grab for the shining light or the light that's shining the brightest, which is, well, use my policy or the service provider's policy, whichever is the most stringent. And I have a problem with that because I don't – it's difficult for me to know what that would mean in any instance. I don't know if (Orrie) and (Jon) have a response to that, but that is something that I'm seeing in the marketplace a fair bit.

(Jon Bancone): Yes, I mean the – you know our vendor response to that is that, first of all, when you say whichever is more robust, that might not be an easy question to answer. Secondly, it may change the nature of the solution. I mean, if the security policy for the vendor is to encrypt, and the security policy for the customer is to put vigorous access controls around something, to say – I'll do what's ever greater, would change the nature of the solution.

If the solution is designed around – we're not going to encrypt, you can't then have a security standard that says – go encrypt. It doesn't work. So, I don't think that – that's why I say that's kind of almost a vague standard. It goes back to the point about vague standards. It's too vague. At the end of the day, what really needs to happen is to spell out exactly what needs to be done in as much detail as you can.

(Jim Harvey): Yes, and I would agree with that. I do think it's difficult in that instance. On the other hand, another kind of real world result of this issue is the gap analysis between the customer's policy and the service provider's policy. I think that's what ought to happen in many instances, if a customer is deciding between the two, but that takes time and money and expertise that, sometimes, is available in a particular organization and, sometimes, is not.

So, I do think some thought needs to be given around the customer security policies, and just be careful of what you – what you ask for. And what I would not – what I would also encourage you to do is be very realistic in your assessment of the strength of your policy.

(Jon Bancone): Yes, (Jim), we have a question here that we can also – that sort of ties right into this, which is …

(Jim Harvey): OK.

(Jon Bancone): There's a question around shared infrastructure and shared services, and I think that, look, there is an element of trust and fairness to the point that if I'm, for example, if I have a server form, right, that I'm doing a hosting services around the server form, and I have specific protocols that need to be in place, because if I change it for one customer, I'd have to change it for the entire environment, then obviously I'm going to have to take on the standard associated with that.

And, another good example would be physical security at a data center. If I'm operating out of a vendor data center, the physical security requirements around that data center are really going to be the vendors. And so, in that context, absolutely, the vendor security standards are probably going to be the ones that you'd go with.

It's not more of – the question asks whether it's more efficient to develop an information security standard, sort of, more broadly. Well, the problem with that is that there are a lot of different standards out there. And, I could have a standard, or, again, the standards can't be vague, right, because then you don't know really what to do. And, you can't design a specific standard unless you know what the solution is.

So you know I agree to the extent that we're talking about a shared environment where the customer doesn't have the ability to make choices, or you're talking about physical security at a datacenter, for example, that you would – you would have a slightly different approach.

(Jim Harvey): Yes, and that …

(Orrie Dinstein): Yes, and …

(Jim Harvey): Go ahead, (Orrie).

(Orrie Dinstein): And even in that example, (Jon), I mean there is still relevance to knowing whether you need specific obligations. And, if you go to a hosted datacenter, you'll see that some customers, for instance, want a CCTV outside the front door to their facilities. Some of them – the door has to be locked at all times with a biometric scanner. You can require dedicated servers. There are a lot of things that you can add into the mix in a hosted environment.

So, while I think it's right that you – the starting point can – always has to be, what is the vendor offering – and some things you just can't change. If the vendor's facility, for instance, is in an urban city close to some bad neighborhoods where there is a lot of crime, you can't say – well, I don't like the location. That would require building a new datacenter. Your option is to pick another vendor whose datacenter is perhaps somewhere in a quiet suburb, which is more secure.

But, some things, again, like, adding cameras, adding more security, adding badge readers or biometric readers, changing some of the configuration to the IT infrastructure, those are all things that you can and should require if they are required under your policies or, again, under any regulatory obligations that you might fall under.

(Jim Harvey): Yes, and I'll ask the hard question here. Clients often raise, with me, this hard question, which is – so, if my policy says, close the doors – doors one through three on the datacenter, and there, in fact, is a fourth door and the service provider knows about it, and I don't, and they leave that door open, what happens? And so, one other thing that I would offer for the audience's consideration and (Jon) and (Orrie's) comments, is this concept of – is there a standard of care attached to what the service provider is supposed to do in the security arena? It's a very difficult thing because, I agree with (Jon), we're all better off the more specific the policies are, but, on the other hand, we don't want to be so specific that we've thrown the baby out with the bath water, if you will, from a – from a security perspective.

These third-party policies, or external policies, sometimes provide that gap filler, but I'll let (Jon) and (Orrie) respond to that standard of care comment and thought.

(Orrie Dinstein): Well, as a customer, you always want some language to protect you because, no matter how long and good your policies are, they're not going to think of everything. And then there's – even if something is stated in a policy, there might be some components of it, which are left to discretion.

And, again, that's where you might end up suffering a loss, a data loss, or some other security event. So, you always want to have some standard, a reasonableness standard, a good faith standard, so that you're – again, you don't have that hidden door that you weren't aware of because you may not have the luxury of doing a site visit before you sign the contract with the vendor.

There are things in their system configuration, which you don't know about. You may not know how many people have administrator access and where all of them are located. And if, for instance, they have to encrypt certain data, but they only encrypt it at a certain point in time. The data is vulnerable until the point that they encrypt it. And, then you've got, you know, human stupidity – the guy who left the door to the truck open while he was driving to the data warehouse and the backup tape fell off the back of the truck.

So, I don't know that anyone is going to have a policy that says you can't be stupid– or you have to lock the door of the truck before you put the backup tape on it. That's a level of granularity you don't usually get to. So, you have to have something to protect you in those cases.

(Jon Bancone): Well I'm not – you know we – there's probably a little bit of area of gray here that we would – I think a vendor would disagree with. I mean, at some level there is a – there would be a you know an obligation to, for example, in your delivery example, would be the obligation to take the data and ship it to the facility – the storage facility – and that would be an obligation.

So, you won't need all the detail around the sub-obligations necessarily. One of the key points here, however, would be that even if you were going to go down this road – I guess there's two points. One is, if you're going to go down this road, you've got to be careful that you can't have the – what has been agreed to – and the non-gap areas can't then be second-guessed as to whether they're reasonable or not, right, because, obviously you know then there's no meat to the standard at all or to the policies that have been agreed to already. So it's got to be only in the gap space. And so, that's sort of an overarching concern for us.

The – within the gap, you've got to also remember – I mean if you hired a consultant to go do an analysis on security, that consultant might give you an analysis around gaps in your security, but they would never – you know and I don't think you'd find a vendor or a consulting company to come in there and say – now, that I gave you this report on where your gaps are that, if I missed something, by the way, I have unlimited liability because my report wasn't perfect. Or, I'm now responsible for the implementation because I did this analysis. So – and there's a fine line there because, obviously, outsourcing is much more robust than consulting, but the point is, you don't want to turn the issue and turn this into something that it's not. So, that's my comment.

(Jim Harvey): That's a – that's a – it's a tough issue. But, let me move – let's move to the next slide because all this ultimately manifests itself in phase three. So, the first phase is – what context are you operating in. The second phase is – what is it that you're requiring the supplier to do and with what level of specificity. And, the third phase is – all right, if the supplier messes up, what are they liable for?

And my high level comment here is that we need to engage in a reasonable conversation. I don't think that either party should give away the store. But, for those of you on the phone that – or on this session, that haven't done one of these transaction recently, and maybe your last one was three or four or five years ago, this is a very, very charged issue for suppliers and for customers and for good reason. But, it's important to engage in a reasonable conversation about what you're asking for from the suppliers.

My second point …

(Jon Bancone): … just the vendors you know the vendor perspective on this is clearly that you know as we talked about the security measures implemented in an environment very based on the sensitivity of the data, the complexity of the environment, the cost of implementing the particular measures. So, you know the view is that the client, through its choices it makes, is in the best position to determine which mitigation measures they're going to take. And the analogy that I always use in negotiations is the security consultant that comes to your house – right – they come to your house. They offer you alarms on the windows, motion detectors, a whole bunch of things, and you pick and choose what it is you want based on a lot of different factors. Cost is certainly one of them. But, in the computer space, in the technology space, it's also network performance, system performance.

So, the customer has got to make those decisions. And clearly, by making a decision, they are, in fact, accepting a certain level of risk. Unless they want to design Fort Knox around their systems, right, they're effectively agreeing, essentially, to take certain of those risks.

And the risk of security breaches already exists within the customer environment. And, obviously, everybody understands that no deployment is going to be 100% effective. There are always risks of gaps, delivery failures and the like. And, the vendor is not in any better – really – you know while the vendor is – yes, they deal in security as part of what they do, they're not really, as compared to the clients, in any better position to control the actions of unaffiliated third parties – right – because really what you worry about here – the primary concern is unaffiliated third parties who seek to get at the information without authorization.

(Jim Harvey): Yes, and I'm going to push back on that a little bit, (Jon), because what the customer is worried about – the unaffiliated third parties – I mean the bad actors, if you will, that are trying to penetrate customer systems are a fact of life. Whether we source or we don't source, we've got to worry about those.

What we're talking about on this slide – and you guys – everyone participating can sense a little tension between me and (Jon) because we've been down this issue several times – is if the supplier doesn't do what it said it was going to do. And a couple, kind of, tangible or tactical points on that – on the second bullet, the compliance with laws and directives issues, your contract needs to not only work on day one but it needs to work on – in year three and year five.

And, if you change your security requirements, or if the supplier comes to you and says – hey, we used to do it this way, but I think we need to do it this way, you've got to have a contract that contemplates that so that you don't have to rewire the whole thing and come in with – attempting to shift costs of all changes forever to the suppliers. Well, I guess they could do it, but they would price in such a risk premium on the front end that you may not want them to do that. But, think about how your policies change, how third party standards change during the life of the contract, and how that works itself out from a price perspective.

But, going back to (Jon's) point about – we are worried about third party activities. I think the customers also need to worry about – and there may be a difference in liability on whether the actor was a third party, or whether it was a service provider, sub-contractor, or employee, or some sort of agent, or representative of the service provider. I think they ought to have …

(Jon Bancone): ((inaudible))

(Jim Harvey): Go ahead, (Jon).

(Jon Bancone): I don't think there's a strong disagreement there. I think – you know look, at the end of the day, you know I think the vendor view on this is that this is a sliding scale, right? The more robust the security, the more liability the vendor is willing to take on. To the extent this is a third party – what I call third party misappropriation versus a vendor misappropriation – clearly there's a distinction in liability in that regard.

But, as the chart points out, there are a whole host of factors, right? We talk about the type of data. So, if it's PII versus non-PII, clearly, that's going to dictate different results. With non-PII, at least at this point, you don't have notification costs to even discuss. But, PII is more sensitive. There's more security around it typically. And certainly, that it's one important factor in determining liability.

So, we've done many deals where we've distinguished the liability based on PII versus non-PII. What type of risk are you worried about? And what's the technical environment? So let me give you an example. Suppose we're looking at a hacking risk. That's the big risk we're worried about in a particular transaction. Well, if the customer has a (VPN) as opposed to you know just access controls around the system you know then you know that is certainly a factor in determining how much liability we're going to take.

If the data – if there – if the big risk you're worried about in a particular deal is the transport of data from one facility to another, if it's unencrypted versus whether it's encrypted, is a significant factor.

So, the type of risk in a technical environment is extremely important in determining this. And, that really emphasizes a fundamental point of the whole presentation, which is you've got to negotiate this stuff in context.

And then, you have all those factors – the type of data, the type of risk, the technical environment. Then, you also have to worry about the type of damages you're talking about, right? We've all – the markets come to a reasonable place, I think, in terms of direct damages.

There's a pretty consistent position in the market on that. Notification costs, third party claims, government fines, loss of profits – they all are different elements and different types of risks, and vendors are willing to take on more or less of those risks independent – depending upon the context and the solution.

(Jim Harvey): Yes, and …

(Orrie Dinstein): (Jim)?

(Jim Harvey): Go ahead, (Orrie).

(Orrie Dinstein): I just want to step in and say a few words about the notification costs because, from my perspective, this clause – the limitation of liability clause – is now becoming the deal breaker in many of these contracts. And, it's primarily due to the notification costs because, as you mentioned earlier, there's 44 states, now, that require notification to customers in case of a data loss.

It's also become industry standard to offer credit monitoring services or other fraud protection services for customers whose data might have been compromised. And there's various statistics out there, but the sort of common number used is $100 per lost record. So, that means that if you have outsourced a certain function or a service that involves, let's say, 10,000 personal records, and they were compromised, then you would, in effect, incur – or someone would incur – a cost of $1 million.

And, obviously if you have incurred – if you have outsourced a million records and they were compromised, now you're looking at $100 million in exposure. And it's that concrete hard number – we're not talking here about damages; we're not talking about claims, lawsuits, all this stuff that we used to worry about in the past and you could quantify and put a risk on it and I'll settle it in a jury and judge and what not – these are hard numbers.

Pretty much the data is lost and somebody has got to send these letters out, and somebody has got to offer relief to these customers, and these are numbers that hit you pretty fast and, again, can become substantial. And, I'm not even talking about the cost of dealing with AG investigations, FTC investigation, class-action lawsuits and everything else – just breach notification and relief for the customers.

And, that's why you quickly get into situations where a transaction could be a $10 million outsourcing deal, and, because of the amount of data, you might be expecting a vendor to take on $100 million or $500 million in potential liability in case of a data loss. And you quickly get into this really big mismatch where people, like (Jon), say – "are you nuts, I'm not going to take on $10 million in profits against $500 million in potential liability. It doesn't make sense."

But, on the other hand, as the customer, you're saying – "look, I'm giving you all of these records, and if you lose them, then surely you don't expect me to have to bear the cost of all those breach notifications and expenses as a result …"

(Jon Bancone): And I agree with that, (Orrie). And, I think that you know there is a strong element here of – that's why I say it's a sliding scale because – look, today, as you run the environment before you outsourced, you run that entire risk. You have no protection whatsoever.

So, there is an element of, if what you're doing in outsourcing – and, again, it's fact specific – but you may be transferring those same employees to me to go run the environment the same way you were running. As a matter of fact, you held me to the same customer security policies that you got held to. And now, tomorrow, there's a data breach that could have happened the day before – the day before you had no protection. So it's not an insurance policy. It's not a complete risk shift. And, at the end of the day, there's got to be some balance to it. Again, the more human elements there are to it, the more risk there is. So that's why you know the easy example is always the data transport because, when you physically move data and you put it on a truck and you have people involved as opposed to a pure you know electronic transmission, there's more risk when you have humans involved. Humans make mistakes.

You know ((inaudible)) so at the end of the day, while I agree with the fundamental point that you know there needs to be some level of protection to the customer, it's got to fit within the pricing and the fundamental scheme of making outsourcing a viable business.

(Orrie Dinstein): That's right. And I think that that's why exactly, as you've pointed out, I think that the limitation of liability clause, in effect, forces the parties to circle back to the stuff that we discussed on slide one, because slide one – that discussion tends to be in the abstract you know here is the stuff that I need. And slide two is here are my policies.

But, when it gets down to the liability, and that's when the vendor starts saying – "wait a minute, I'm not going to accept these kinds of numbers," -- now you start saying – "well, how much PII am I giving you and why? Maybe I can keep some of that PII on my side of the fence and not give it to you. And, if I am giving it to you, then, again, maybe I need to encrypt it so as to not incur these potential expenses. Or, maybe I need to pay you a little more and have you encrypt it."

And so, I actually find it fascinating that the limitation of liability clause is, in effect, reopening or forcing the parties to go back and look at the operational and security components and starting to really revisit the transaction with a new lens, which is somebody is going to pay a lot of money if something bad happens to this data.

So, given that the vendor is not willing to – and, by the way, I would caution people on the call – some vendors just sign a blank check and say – "OK, I'll take unlimited liability" – those are usually not the IBMs who can afford almost unlimited liability; those are the vendors that have a very shallow balance sheet and really can't stand behind that commitment; and it always scares me when a vendor just says – "OK, I'll take your unlimited liability clause." So …

(Jon Bancone): Yes, this – I guess the point I'd make there, (Orrie), is that if you're deciding – you know I would look at it this way. If I'm a – if I'm a customer – and I am not a customer you know I don't represent customers – but it seems to me you can't look at the terms of a contract outside of context. So, if you're looking at the package and you're comparing the package of here what one vendor is giving me versus here what another vendor is giving me.

If a vendor is giving me unlimited liability protection, but their solution is not robust, I'm not sure you're better off as a customer to have a less robust solution even though you've got the liability protection versus a more robust solution but less liability protection. And, so you've got to always, again, fundamentally, got to go back to context and look at what's happening.

The other point I'd make out is – I'd say is that is – what you just said is exactly why we encourage the security teams to talk early on, because we don't want it to come down to – you've been negotiating this deal for three months, and now all of sudden you're going to go revisit the solution. That makes no sense.

You really want to get the security teams out in front of the issue. And, we've found, by the way – we have done that in some deals and found that it does facilitate a better discussion, a better solution, and an easier discussion when it comes to liability.

(Jim Harvey): For everyone on the call, we've got about five minutes left. And so I would encourage you, if you've been holding questions, put them in the chat box and we'll try and get to them in rapid-fire fashion.

While you're doing that, I think both (Jon) and (Orrie) have made good points. A couple fundamentals – (Jon) talked about the fundamental analysis here. A couple of fundamentals – go back, this is the back of your documents that may have been set in stone for a number of years, but they need to be re-read because, in this new data world, what constitutes a direct damage versus a consequential damage, (Jon) and I could drink several rounds of adult beverages arguing about whether regulatory fines constituted consequential damages or not. But, those need to be rethought and revisited in light of this.

The other thing that I would encourage everyone to think about is looking at the responsibilities of who does what if there is a data breach. So, your clauses about audit – do they properly contemplate the forensic activities that you and/or your card issuer and/or law enforcement may want to embark upon? And does your third party provider, IBM or whomever else, participate in that? Who pays for it? How quickly do they open your – their doors to allow you in to do it? All those sorts of things need to be thought about in advance.

I've dealt with situations where that was agreed to in the contract and where the contract was absolutely silent. When you have a data breach, it is helpful to have that list of responsibilities in the contract and thought about, and negotiated, quite frankly, in advance.

So, I don't know, (Jon) and (Orrie), any concluding thoughts? We've just got two or three minutes here, and you guys have been amazingly helpful and insightful – so much so that we don't – we don't really have any questions. But …

(Jim Harvey): … I'll give you guys a couple – the last word.

(Orrie Dinstein): Yes, I'll just say this. I mean, as I said before, this is becoming the thorniest issue in contracts, at least, from where I'm sitting. And, it definitely requires a lot of common sense and a lot of thinking through of the issues very carefully.

The days of just saying, unlimited liability or five times fees paid under the contract or just throwing out a number, I think, are gone because, again, you can't just assess things in a vacuum, and, at the same time, you can't just dump everything, and, I'm helping (Jon) here, but you can't just dump everything on the vendor and say – "you're going to be responsible for everything, and I'll do nothing, and sign on the dotted line," because, again, you're not going to find vendors to sign that, and those who do, as I said, can't stand behind those commitments. So, you need a lot of cooperation and a lot of common sense to get over this one.

(Jim Harvey): (Jon) you're – you get the last word, sir.

(Jon Bancone): I usually don't, by the way, but I would say this. Look, at the end of the day, the most important message that we can drive here, I think, and we all agree on, is that you've got to get out in front of the issue early. You've got – you know what we typically tend to do on the vendor's side is we literally analyze each element of the solution and the risk, and decide what mitigation measures that we think you know – that are being proposed are, and where that significant risk lies. And we designed the solution around liability in that context.

And the earlier you can get out in front of the issue, the earlier and – the earlier in the process that the security teams can talk, I think you know it leads to a much easier discussion. And, look, if you're a small company and you don't have a security team, there is somebody at the company that makes decisions on security. So, even if there's no you know major security team there, having a detailed discussion about what you want to do and how you want to operate in that environment in the early stages of the deal is critical to getting the deal resolve in a short time.

I think, at the end of the day, the goal of both companies is you want a reasonable contract with reasonable liability approaches with you know – you know sitting across the table from people that you can you know work out issues as they come forward, because these deals, the outsourcing deals, tend to be longer-term deals. So, you're – it's not like you're dealing with the person you're negotiating with and you're not going to be sitting across the table with them the next you know month or two to discuss something else. You want to try to resolve these in a fair manner but also in a positive sort of light.

(Jim Harvey): OK. That being said, thanks everyone for joining us. We'll have a bunch more content this year at the IT E-Commerce and Privacy Committee and, otherwise, through the ACC.

And I'd like to thank each of you for joining us. And, in particular, I'd like to thank (Jon) and (Orrie) for taking time out of their busy and valuable schedule to give us their thoughts today.

(Kelly), you may need to do the final rights here on recording and everything.

Operator: Thank you, (Jim). Just a final reminder to our participants, if you have any additional questions, you may still send them in the chat box. We appreciate your participation and you may now disconnect.

END