SmartPros
Legal & Ethics

ACC Association of Corporate Counsel
The in-house bar association.℠

Data and Information Security: Friend or Foe?

Data Information Security: Friend or Foe?

MARNI CENTOR: Hello everyone. The Association of Corporate Counsel and SmartPros Legal and Ethics welcome you to today's webcast, "Data Information and Security: Friend or Foe?"

[*The instructions provided here were intended for attendees of the live webcast when it was originally broadcast. You may submit questions and comments regarding the content of this course using the Questions and Comments link on the left side of your screen below the video.*]

Our presentation today will be moderated by Julienne Bramesco, general counsel for Colonial Parking. And now, I'll turn it over to Julienne.

JULIENNE BRAMESCO: Thank you, Marni, and welcome everyone to ACC's Small Law Departments Committee presentation, "Data and Information Security: Friend or Foe?" sponsored, again, by the Small Law Departments Committee and our sponsor, Meritas. We have a great program today. We have two wonderful speakers: Rob Kleeger, who is the managing director for The Intelligence Group and Fernando Pinguelo with the law firm of Norris, McLaughlin & Marcus, P.A.

We're going to start the presentation with some basic facts, and Rob is going to set the scene for us, but first I'm going to turn this back over to Marni for the first verification code.

[*The CLE code provided here was for use only by attendees of the live webcast. To obtain your CLE certificate for this archived webcast when you have finished listening to it, click the EXIT COURSE button at the top right of the screen to return to your My Courses page and then click the certificate link or icon beneath the course listing. In the pop-up window, select the desired jurisdiction from the drop-down list and enter any requested data, such as your bar number and the CLE code that popped up while you were playing the archived webcast. (This code is required for New York and Ohio attorneys only.)*]

ROB KLEEGER: Good morning, or afternoon, for those of you who have attended. It is a fact that today's modern life has an enormous volume of information which is created, exchanged and stored electronically. Those conventional documents which originate as computer files, where e-mail is now taking [the] place of both telephone calls and postal letters, and many if not most commercial business activities are being transacted using computer-based business process. In the past decade, we've seen, read or heard about the breaches of data and data information security. Today it seems almost daily another organization reports some type of security breach that has occurred. Once seen in only the larger organizations that involved sophisticated technologies, it is now seen routinely of all size businesses and all various industries.

Data breaches last year were estimated to have cost businesses some $1 trillion, and the Heartland Payments Systems kicked off 2009 with the disclosure that they'd suffered perhaps the largest data breach in history. And just the other day, Alberto Gonzales, a hacker previously charged in at least three other federal cases, was indicted by a federal grand jury in New Jersey yesterday on charges alleging that he and two co-conspirators located in Russia hacked and stole credit card and debit information of more than 130 million people. So the bar is set pretty high. The indictment alleges that those people affected had their transactions processed by Heartland Payment Systems, which is one of the largest credit and debit card processing companies in the world.

So, let's find out a little bit in terms of data security. And how is data security defined? I've asked many people and also did some searching online, and if you find those surveys, you'll see that you get many different answers. As these sources will indicate, you'll know that data security is simply keeping sensitive information from falling into the wrong person's hands.

Here is a short list of some business and legal reasons [with] regards to having safeguards in place for data and information

security. Fernando will discuss some of these in a few minutes, typically addressing the top legal issues that businesses are facing today. From a technical perspective, as well as a business perspective, I'd recommend the general rule that every business, regardless of size, that maintains computerized records containing personal information must employ reasonable safeguards to protect it.

Based upon my experiences in many different corporate investigations, there are many different risks, but I simply want to highlight just a few: workplace, lawsuits, trademark infringement, patent infringement cases, the electronic viruses that exist. Some additional risks are class action lawsuits, reputational risks, shareholders, media, and oftentimes e-discovery would be a risk that corporations of all sizes may face.

JULIENNE BRAMESCO: Rob, my company is a low-tech business, pretty much. I mean, we're a parking company. We park cars. What kind of intellectual assets would a company like mine have and what kind of intellectual assets do nontechnical companies have?

ROB KLEEGER: That's a great question, and I guess it really comes down to: It depends. Many times we'll be involved reacting to some type of an investigation. Traditionally you would think that customer lists, software code, any information in terms of credit card transactions that you, Julienne—that your business may use as a parking garage—could potentially be a target of some type of attack or breach. It really depends on the nature of how much of this business you maintain these records and then really how your business is set up. Believe me, we're in a business that routinely is reacting to the very simple things that you would imagine a customer list should be protected and have certain controls in place, but quite frankly aren't, and we're brought in after the fact when an employee is now at a competitor and we find that they've taken some of those clients over, even though these are things that are normal and routine in many businesses. It really varies according to the size, the business, what that business does, how they operate, etc.

JULIENNE BRAMESCO: But it's really not overstating the case to say that really every business is going to have some types of intellectual assets that need protection.

ROB KLEEGER: Absolutely, and the exercise is to pay close attention to those things and go through that exercise of: What are those intellectual assets that you may think might not be important or valuable, which we're going to cover in a few slides ahead—how to think about those types of things, and adding some value that either the corporation may decide is not of value if it ends up in the wrong hands, whereas you might identify that there is information that your business collects, and if it was to end up in the wrong hands, what the risks and the concerns that can occur [would] be. It's really just a matter of taking a step back type of na approach. Oftentimes the investigations that we're involved with, we result in proving that those intellectual properties that are not often protected or properly secured should have been in the first place. Many times it's simply the individuals—the people that we employ, the human beings—that are the cause of many of the biggest risks.

So, why are these intellectual assets difficult to secure? Some of it is because this information literally could be anywhere. We're dealing with, typically, paper records and documents—electronically stored information or ESI. It could be found on servers, PCs, laptops, smart phones, flash drives, home PCs of your employees, but many times it's simply in the heads of those employees. Many times some of these phrases you may recall hearing or may have even stated some of these things yourself:

"Nobody would ever take that, and if they did, so what?"

"Our employees absolutely do not steal."

"The competitors—they can't steal because we have firewalls. Besides, only hackers and other hooligans are going to try to break in."

The reality is: These are the types of things that are happening and unfortunately happen more often, and it's after the fact, when somebody assumed that no one would have any value to that type of information, you learn that that is, in fact, the

information that has been breached.

Getting to some facts, there's a survey that's going into its 13th year that's put out by the Computer Security Institute. In 2008, their survey of over 522 computer security practitioners from various private and public sector corporations, governmental agencies, financial institutions, medical institutions [and] universities have revealed that more than half of those organizations that employ less than 1500 [people] are the ones that are causing the biggest threat. You'll also note, on the right hand side, the percentages of that demographic of the survey as well. What also is interesting of this survey is that 32% of the respondents were senior executives with the title of "chief" something. This is a pretty big indication that there are definitely controls in place, regardless of the size of the organization, that security is an issue.

Some of the findings that have been probed were that the most expensive computer security incidents were those that involved financial fraud, where the average reported cost was close to $500,000. The second most expensive, on average, was dealing with a bot computer or viruses. A bot is basically a computerized task or program that will automate doing things such as sending spam to blast Web sites off of the Internet. It could do denial of service (or DOS) attacks. It basically could take over your computer without your knowledge and use that computer for conducting some type of unlawful activity. Again, viruses, incurred frequently, and as a point of interest, dealing with loss of either proprietary information or the loss of customer and employee confidential data averaged at approximately $241,000 and $268,000 respectively.

This is kind of the big shift where we're starting to see computer crime become a lot more organized and professional. What that really means is that, in the past, one of the things that the perpetrators were doing were motivated by bragging rights. Today it's no longer by bragging rights; it's about money.

Oftentimes we're speaking to corporations of all sizes, and sitting around a table where their general counsel, their HR [human resources] directors, their IT [information technology] directors, the business executives, the CFO [chief financial officer], the CEO, etc., and you'll find that in this survey that there were 53% [of] the organizations [that] allotted only 5% or less of the overall IT budget to information security. [This is] counterintuitive, but what is interesting is that, increasingly, security is viewed as a problem that is far broader than technology alone, and in many instances it's part of the security budget, where it comes from the audit as well as the legal departments.

FERNANDO PINGUELO: Thank you, Rob. As Rob indicated earlier, there are a variety of federal and state laws, as well as common-law protections when it comes to securing data. Frankly we can spend an entire seminar on each one of the laws listed in Rob's previous slides. What I've done, from the legal aspect, is [to] select the top seven issues that are confronting businesses when it comes to electronic data preservation and obligations related to electronic data.

One of the most common issues that I'm confronted by in inquiries from clients is this theft prevention act. Many states have enacted an identity theft prevention act similar to California's act. Basically these statutes require businesses to protect what's deemed to be private information from disclosure, and if there is disclosure, then it requires certain notification obligations. When you're dealing with identity theft prevention act issues, the threshold question relates to what is the private information or personal information that must be protected as Rob indicated earlier? The acts generally define personal information as an individual's first name or first initial and last name linked with any one of a variety of data elements, including Social Security number, driver's license number or state identification card number, or account number or credit or debit card number in combination with any required security code, access code, or password. So to recap, you need a person's name, first name or first initial and last name plus any one of these other factors.

JULIENNE BRAMESCO: So it's a combination of factors, Fernando?

FERNANDO PINGUELO: Correct. It's the name plus any one of these other factors—Social Security, driver's license number, etc. That's how it's defined, so if the information that's lost or it there is a breach related to the information doesn't have this combination, then it wouldn't be found under this act. There is a caveat to that general proposition. To the extent that the information I just listed—again, name, Social [Security number], driver's license, etc.—is separated in a variety of different databases, if the information can be linked together somehow through the breach, then you do have an obligation to notify the individuals implicated through some sort of a notification.

Once you've concluded that the information that has been affected falls within the statute, then the next thing you need to determine is whether or not a breach has occurred. The statute defines a breach as "unauthorized access to electronic files containing personal information, as previously defined, that compromises the security confidentiality or integrity of personal information when access to the personal information has not been secured by encryption." In other words, many businesses will have encryption codes that would prohibit general access to the information, so if you don't have such an encryption code, then you could be subject to this notice provision under these acts.

Once you determine that personal information has been implicated and there has been a security breach, then the statute continues to identify what needs to be done in terms of notifying either your employees or your customers that there has been a breach.

Let me give you an example of what's come to my attention recently. One of my clients, during a routine audit, determined that they could not account for 90 backup tapes. They just didn't know what happened. There was a time when they moved a few years back, and that could have been a place where they could have lost them or misplaced them, but they just couldn't do it. So I had to take them through the act and determine whether or not they needed to notify their employees, because there was a potential that the information could have contained this personal information. So I took the employees through a series of steps to investigate what happened and determine whether or not there was a breach that needed to be reported. After interviewing employees and conducting an internal investigation, we concluded that it was not necessary. So these are the kinds of steps you would have to go through if such a situation were to happen to you. Fortunately for the company, we didn't have to go through the next step, which was notifying the individuals.

JULIENNE BRAMESCO: How likely does the breach have to be Fernando? Is it: We can't find something but we're pretty sure we have it? Or is it the poor guy whose computer got stolen from his car; we know it's gone?

FERNANDO PINGUELO: There's no bright line. If you can show due diligence, if you can show a proper investigation—a thorough investigation—typically involving interviewing employees, tracing the steps or trying to locate logs of data collection devices, etc. If you can show the steps that you went through to determine that the information that was lost was not likely within the purview of the statute, then you're in pretty good shape. But again, that would require internal investigations and documenting each step. Sometimes, and in this particular case, we actually suggested and the client did hire a private investigator to interview some people as well, just to show some objectivity. Because the cost would have been so much greater to notify the employees, we wanted to make sure that we had a sound judgment on the lost data.

JULIENNE BRAMESCO: That's pretty scary stuff. I just want to remind everyone that you can ask questions to the panelists by using the question tool on your control panel.

FERNANDO PINGUELO: Typically, what these laws do—and I'll go over the other six remaining laws—they protect information, so clients will want to protect confidential information. That typically includes trade secrets or client lists, intellectual property, personally identifiable information, health and financial information. Typically, we see these issues come up in a situation where an employee who has access to this information—either intellectual property or confidential information—either is looking to switch positions to work for a competitor or sometimes we see a situation where a company will change the terms of an employee's employment so significantly that it causes the employee to search for a new job and perhaps even work for a competitor. So if your company is engaging in any sort of changes like that that affect employees with access to sensitive information, it's important to be conscious of the fact that at times employees will begin to download some of this information, and you want to be sure that you're monitoring that activity.

JULIENNE BRAMESCO: One thing I've learned, particularly as a labor and employment lawyer, but even here as a general counsel, is that when you're looking at employee terminations or any kind of employment action, it's really important to get your IT people involved and to figure out what to do about security and computer access.

FERNANDO PINGUELO: With that, I'll turn it back to Rob to continue on the technical aspect of the presentation.

ROB KLEEGER: Great. In terms of talking in line with the data breaches, the additional surveys that are out there—there's one from the Phenomenon Institute, or the PI, and the PGP Corporation, again, have been putting out surveys like this for several years. The average cost for a breach per customer record in 2008 is $202. Now I've been monitoring these surveys for the past six years, and every year it increases. So the average and the annual cost, based upon a data breach study that tracks a wide range of cost factors that include the expensive outlays for detection, escalation, notification and response, along with legal as well as investigative and administrative expenses that come from customer defections, lost opportunities, reputation management, as well as the cost associated with customer support, the setting [up] of hotlines which is also a part of some of these statutes, as well as credit monitoring subscriptions if a breach was to occur and it was reported. There was an obligation to set up so that those things don't happen again or at least had a good faith step and a reasonable step for the employers or those potentially who have been the receivers of such breach to set up those hotlines and monitoring subscriptions.

What was interesting was the average total of per-incident cost in 2008 was $6.65 million compared to the incident cost of about $6.3 million in 2007. And it has to deal with the reflection of sensitivity of the data from the customers and that the third-party organizations accounted for more than 44% of all cases in 2008, where most frequently the cases of data breaches were due to additional investigative and consulting fees that were caused from insider negligence, which the study shows was about 88% of all of this year's cases were based upon insider negligence, which in essence is this information, talking to Julienne's point of customer records, by not properly going ahead and having the safeguards in place was where the neglection occurred, which was the increase in the expenses based upon these breaches.

JULIENNE BRAMESCO: So these are all preventable expenses?

ROB KLEEGER: These are all very preventable expenses, absolutely. Everybody, or most people, I would imagine, at this point in time are familiar with the TJX breach. In June of this year [2009]—and again these are all very recent occurrences—the owner of TJ Maxx and Marshall's, the TJX Co., agreed to pay $9.7 million in a settlement with 41 U.S. states, including Florida, over a 2007 computer breach that left millions of consumers vulnerable to identity theft. This was a multistate investigation that was triggered by the largest computer security breach ever reported. So it's kind of in your face on a daily basis, and this is something that the bar is now set [to a point] that you would think is pretty high. These are the things that unfortunately are where when you are working overseas with other conspirators. Who knows when the next one is going to be? The bottom line is that some of the most sophisticated firms have had a breach, and it doesn't make a difference whether you are one of these household names or your firm could potentially be next. It really comes down to simply the way that you do business and the types of information that you collect, and how you maintain that information could be a critical target.

This is a slide that I use in many a presentation, and it's what keeps inside and outside corporate counsel asleep at night, and reasonably should. It really shows that depending upon how your business functions in relationship to using technology, the flow of business operations, how you interface with your clients and your employees, both inside the corporate enterprise as well as outside, it could be a very troubling statistic. My recommendation is: If you don't have one of these, you absolutely go ahead and you try to develop one—to do a data map. Know your business flow. Know your operation. Know where this information may in fact exist.

JULIENNE BRAMESCO: Not only am I up at night, but this is giving me a headache. Can you walk us through it a little bit Rob?

ROB KLEEGER: Sure.

JULIENNE BRAMESCO: What is it that we're looking at?

ROB KLEEGER: In essence this is something that is commonly asked. Is this a large organization with multiple locations—international—or is this a small business? The reality is: It depends. Depending upon how your firm does business—for example, let's just say that over here is the corporate headquarters where your IT is. And the way that you do business—Julienne, for your business, for example, you might have multiple locations, and at each of those multiple locations, you're

going to have computer equipment. And you're going to have individuals that are going to process this data, and they're going to transfer this information from this location to that location—all over the place—which is really what these little fine lines are showing, is that around the entire world, the way that you're transacting business, which many times is automated—you scan a credit card through to pay for the parking of my car in your garage—is going to touch upon multiple systems.

Who are the people and what are their job functions? Do they have access to all of this information which [as] Fernando [said], going through, that you need your first name or last name, your Social Security number, your credit card information, your CVV code, which is that three-digit code on your credit card? Whatever everybody is familiar with, when you're asked those questions when you purchase something electronically [with] a credit card, whoever has that information—and let's just assume it could be on a laptop that gets stolen. This is the level of detail that you need to know, so that in the event a potential hack occurs, just because it's a hack doesn't necessarily mean it's a breach. It doesn't mean that you need to go through those simple steps that Fernando had to go through to take their client to determine, and that we routinely will take clients through [in] an investigation, to hope that it's not a breach. And those are the types of things that you really need to be prepared. So this map is really something that depends on the size of your organization. You really need to get familiar with these types of things, not only from a breach standpoint, but from the e-discovery standpoint and just from the standpoint of just knowing how you need to collaborate with other pieces of your business. It's not solely IT's responsibility any longer to know how your business operates.

JULIENNE BRAMESCO: I think that was the real eye-opener for me as I went to a program on e-discovery. And they said the federal judges expect that lawyers know something about data and about the computers and the fact that "Well, gee, I'm just a lawyer and I don't know anything about this," is just not acceptable any longer.

FERNANDO PINGUELO: Those are great points, and as outside counsel, every time, whether I'm doing work for a client on the compliance end or establishing policies or whether I'm handling a full-blown litigation, with every client I need to engage in a discussion with in-house counsel and their IT director on where servers are located, where PCs are located, and [where] a variety of hardware are located.

To give you a concrete example, I was involved in a 20-day trial in which we had our IT person on the stand for two days. Would you believe on the night before the second day of testimony, the IT manager had a nightmare and realized that there was a backup tape he failed to disclose back in a closet in California? So, as you can imagine, in the middle of trial, with two days worth of testimony, this was a complete shock, and we had to go through a variety of steps to ensure that the other side was given access to the tape. We had to fly in the tape. We had to make copies and etc., so it was a costly endeavor because of this forgetful person.

But the reality is: I'm finding, as I deal with IT people, their worst nightmare is losing data. So what happens? They backup and backup and backup, and they've got tapes in their trunk, they've got tapes in closets, etc. So as outside counsel and as inside counsel, you really need to get a hold on what is out there in terms of inventory and where they are being located, so that something like this—having a nightmare realizing that there is a backup tape that they forgot to account for in a closet in the back office—doesn't happen to you. This is a scary slide just simply because it can certainly be burdensome and time-consuming to understand the system, but once you get it place in a neatly focused protocol, then it's much easier to deal with on a day-to-day basis. With that, I'll turn it back to Rob on the technical [aspects].

ROB KLEEGER: Right, just for the sake of time and to keep the presentation moving. So, where does this information live? Again, the data map that you saw just a slide ago is there to represent the laptops, the desktops, the servers, the voice over IP systems, your smartphone devices, your CDs and DVDs, the thumb drives that exist.

But what about your iPods? Some organizations will absolutely have their iPods that are allowed at their offices, and an iPod is nothing more than a hard drive that you can download information to—not just songs—and there have been many situations that I've had where the theft was committed using an iPod.

How about copy machines? This is something that—I was on WNBC on a report cast that was talking about ID theft. When the mortgage industry, before it crashed, before the financial industry started to crash, well, guess what? All of your—let's

just say it's your mortgage, paperwork, all that documentation—think about [the fact that] you're going to have a person's first name, last name, their Social Security [number], their address, their last five addresses, the mother's maiden name. Everything that you need to fill out on an application is now put onto an electronic device, which these digital copiers, which have hard drives in them, which are connected to a network that many times [isn't] as secured as commonly IP might think that they have been, but they haven't been. They're plugged in and sometimes IP doesn't know about it, because it's not their territory. They're not into the main control of digital copiers. That's facilities or records management. But they plug it onto their network and it's not being monitored. And guess what? That's where your breach could occur and that's a target. You just think about knowing where all of this information is, and that is really kind of the lesson learned is thinking about all of those types of things.

Let's just go into some of the basic things that you should start to inventory by identifying all personal information, both paper and electronic, just know where this information would be. Identify all the contractors and vendors and other service providers that you maintain. Do they maintain any type of personal information? Sometimes you're outsourcing a payroll function or HR function. How are they maintaining their records? Is it in a file room that anybody can have access to, and it's your employees? Those are the types of things that you need to take control about.

Evaluate different work alternatives or work arrangements. Today it's very common for people to have more life balance that would enable them to work from home or remotely. Those types of things are fine, but just as long as you know that that person's job function; are they going to be walking around with a laptop or using a home computer that's going to maintain client information that's personal of nature that could potentially be a breach? The issue is really just a matter of identifying how your business operates. And more often than not, I find myself reacting to a situation—putting Band-Aids that have been there all along—to then sit down based upon the pain and costs involved where there were certain very preventative, easy, basic, fundamental steps that corporations could have taken to avoid or mitigate maybe some of that cost. And that's really what I'm recommending, is [that] you take a step back and you really relearn, because just as much as you have a policy today, it doesn't mean that people are consistently following it and it doesn't mean that there aren't new policies being created that are out of your control. It's very important to get a handle as to this type of information.

There are some cost effective security tips. One of the things is: If you don't have a security plan, get one. If you do have a security plan, then that's great. Think about the short term, the long term, and most importantly the ongoing. Look at that thing every quarter [or] every six months, depending upon the nature of your business. Always take that out and look at it and see what has changed in your business. As technology increases rapidly, companies adapt to the technology, but they're neglecting to put that into their security plan. Define how much is enough? How good is enough? Accept the general rule of thumb that I call good security equals compliance. However, compliance doesn't necessarily mean that you're going to have good security.

Fernando?

FERNANDO PINGUELO: Yes, briefly, the second hot topic that I'm finding clients dealing with is securing their data on endpoints. Time and time again, I'm confronted with clients who use their own personal memory sticks instead of using a company-issued stick, so they're using these memory sticks with personal information on them, etc. This causes a problem from a compliance point of view and a legal point of view, because how are you supposed to manage these data storage devices if they're being used personally?

Another issue that has come up relates to e-mail capacity. I had a client who has a policy where it significantly limits the e-mail capacity of its employees, so they're only allowed to send and receive attachments to e-mails in a limited capacity. So that, on its surface, may sound like a great idea. They're trying to save some storage space, etc., but practically speaking, what winds up happening is: Employees, since they can't send this data over the e-mail, they'll start saving it on their individual hard drives with their laptops. So this wasn't an issue; I guess the company knew this was going on, but they didn't think much of it until a key employee left his laptop in a car that had been stolen. There you go; you're now losing a variety of data because a particular policy that was in place and sounded reasonable on its surface, but people were circumventing it because it really didn't adapt to their daily duties. That's an example of how endpoints can be breached and there can be security breaches simply because you have a policy that doesn't quite fit the day-to-day expectations of an employee.

JULIENNE BRAMESCO: I don't do this now, but awhile ago I used to actually e-mail myself documents to my home computer so I could print them out and work on them at home rather than carry them back and forth, and I realized—it came to me—what a horrible nightmare that could be both in terms of breach and in terms of finding the documents if there was ever an e-discovery request. So I don't do that anymore.

ROB KLEEGER: That's smart. Oftentimes what IT does, to Fernando's point, is that they do put some type of measures of limiting their storage boxes of their e-mail. They're creating Yahoo! accounts or Web-based e-mail accounts that are not being monitored, or if it is, it might only be monitored to the point that we're blocking Yahoo!, but we're not blocking Gmail or Google. They need to know that they need to block those specific addresses, so that you can't send Web-based e-mails, not just you can't use the Internet for searching. So again, these are very complex. It could be another seminar for another day. I think the point is knowing what your data is, knowing the data at risk, which is really what this slide is.

A very simple thing that I've done many times before is value what type of [information this] is. If you can add and attribute some type of value to having that credit card number—if that was to get into the wrong person's hands, is that credit card number something that would be a high value, five? And if that exposure level was to be a breach that came through our organization, if you multiply the two, you're going to now have a risk level. Based upon having certain levels, you set up a hierarchy that, if it's in a range between one to five, then maybe you're just monitoring those types of data security risks. If it's a level between six to 15, not only are you monitoring it, but you're putting some type of access controls in place. You're putting some type of protection or policies based upon the work flows in place. You're putting a couple of different levels or layers of security. If it's a degree of risk of, let's say, 16 or greater, either replace the methods or put stronger encryption methods in place, or whatever, depending upon the nature of the data that you're trying to protect, with all being reasonable in terms of the solutions that are out there to serve the purpose of your size organization to avoid that risk.

It's really simply going ahead and valuing each independently, as well as if the individual was to have a breach or a hacker came into our system, and we have a database of comingled credit card, Social Security, CVV and personal information together, and they had that, like in a case like a TJ Maxx, think about the repercussions and the costs involved, regardless of the size of the company. Because basically you're out of business if you're a small business and that happens. Do some simple math and assess the value.

Once you have identified and you've valued those risks, this next graph is kind of a four-quadrant grid that basically will show you what you need to do if the information that somebody was to gain access [to] is a high [value] information and it's top-secret information to the company and it was to get into the wrong person's hand, if there's no regulatory action or there's no compliance reason for maintaining that data, destroy it. Once you've gotten paid, again, depending upon your business and whether or not there's an overseeing agency, you might not want to have that information any longer. Depending upon the level of degree, as to whether or not it's in the wrong person's hands, is whether you'll choose to destroy it, you'll go ahead and ignore it, you can either monitor it, or just secure it.

As far as in summary, whether an individual works for a multinational powerhouse with branches around the world or at a home office, a sound information security plan really depends upon applying some basics. Take stock of the information that you currently have. Look at and understand the threats. Identify some type of value in order to protect those types of risks and threats. Have a preventative program in place that may either be an incident response plan that will maintain records and audit trails and logs of card access or surveillance systems or monitoring—not only just the IP side, but the physical security layers as well. Overt or covert is simply a matter of style, but ignorance is just one of those things that today is not going to stand up well in front of a judge or in the media.

So I close with this slide, which basically is a cartoon that illustrates today how businesses are commonly run. Think about what could occur if the information contained on your electronic devices, both at your home as well as the workplace, if an individual at your organization was to lose it, it was to get stolen, or it was to be breached.

I appreciate your attention and listening, and I will have Fernando take through the next portion of the slides.

FERNANDO PINGUELO: Thank you, Rob.

JULIENNE BRAMESCO: Fernando, I'm fascinated by your next topic, because I think we get weekly questions on the ACC listservs about social networking sites. They just raise so many issues, so I'm really anxious to hear your thoughts about that and how they relate to data and sensitivity.

FERNANDO PINGUELO: You and me both. This is probably the hottest topic that I'm getting on a weekly basis. I could break the social networking sites issues into at least four components: HR issues that arise with social networking sites, lost productivity issues with employees working and surfing the net instead of working, security breaches, and finally cyber-snooping.

Let's focus on the employee/employer issues—HR issues. I'm finding a lot of use of social networking sites to harass fellow employees. Sometimes employers will make hiring decisions based on information that they find on a person's MySpace account. To give you an example, if you can't discriminate against a person based on what you can see on a resume, you certainly can't discriminate against a person based on information you see on a social networking site. What you find with social networking sites—you're being provided information that you wouldn't normally be privy to. Sometimes you may have information that a person is pregnant or has a medical condition that you wouldn't normally see on a resume. You can't base your hiring practices based on information that you typically would not be able to use against an employee. So we see a lot of that.

A lot of times employees will use social networking sites for collective bargaining gatherings and discussions or to complain about an employer. Again, you can't take an adverse action against an employee just simply because they're using a method that traditionally they hadn't used before.

The second issue relates to lost productivity and that's self-explanatory. If an employee is surfing their Facebook account instead of working, there are going to be issues that are going to affect the bottom line eventually. Security breaches: The headlines often occur that you will see viruses that are incurred because of improper use of social networking sites. Also, what we're finding is: Because social networking sites are a very informal, short way to communicate, employees are disclosing confidential information to others in the outside world unwittingly, so that's an issue that we're running against.

Finally, cyber-snooping. There's nothing necessarily wrong with cyber-snooping. Cyber-snooping: That is using Internet to gather information about employees or competitors.

JULIENNE BRAMESCO: Or your teenage daughter.

FERNANDO PINGUELO: [There is] not necessarily anything wrong with that in and of itself, but when you take it to a degree that affects federal statutes that are out there, then it could really put the company in a difficult position. To give you an example, recently in New Jersey in federal court, the restaurant chain Houston's was involved in a case of cyber-snooping that crossed the line. In that particular case, a manager gained access to an employee's MySpace account by allegedly coercing an employee to give the access code, so this was not a readily available MySpace account. You needed an access code and needed to be invited in order to observe what was going on in that site. Lo and behold, the manager obtained the access code and then accessed that particular employee's chat room and they found some nasty stuff about management and customers, and the employee was fired. The employee filed a claim under the Federal Stored Communication Act and prevailed in the end.

This is a very tough act in that there are mandatory minimums for damages and attorneys' fees may be awarded. So in that particular case, the company crossed the line by coercing—a jury did find that the employer did coerce the employee to turn over the password to gain to the MySpace account of another employee. That's certainly the four areas that I'm seeing implicating businesses.

The lines are often blurred because companies often encourage the use of online social networks to conduct business or to

communicate with employees or customers. You have to be careful. If you're allowing it on one end, you've got to be sure that it's properly being used.

The next issue that I'm seeing a lot about relates to preserving electronic data, and I didn't want to spend much time on electronic discovery, because this is the slide that talks about it, but I do want to touch on a couple of quick points relating to obligations to preserve data. We all know that we're all obligated to preserve data when a lawsuit is filed, but the law also requires preserving data when you anticipate that a lawsuit will be [filed], so that's where we're seeing a lot of activity—clients giving us calls on whether or not they should be issuing litigation hold notices given a particular issue that has arisen short of the filing of a complaint. That's a highly fact-sensitive analysis and we really need to know a lot about the situation in order to recommend whether or not a litigation hold should be affected. Litigation holds can be costly, so we're very careful not to impose undue burden on the client in that respect.

Metadata issues are increasingly affecting clients. For those of you who aren't familiar with metadata, metadata is data about data. Essentially, when you create an electronic document, whether it be a word document, Excel spreadsheet, etc., there's a variety of information contained within that document that may not be visible, at least superficially, that can give a whole host of information to a variety of people. Typically, metadata is not compelled or not required to be disclosed in a lawsuit unless specifically asked [for] or there's a reason for it. But what's happening is: Parties, in order to drive up the cost of litigation to encourage settlement, are asking for this type of information routinely.

JULIENNE BRAMESCO: I actually loose leaf over metadata because I think, for many of us who are in-house counsel, anytime your clients are sending documents to you, you're affecting the metadata. Isn't that right?

FERNANDO PINGUELO: Correct, it alters the information. Correct. To give you some examples, where metadata really comes into play, we see a lot of it when you're negotiating contracts. Let's say there are a variety of versions of drafts that have gone back and forth, and if there's an issue with a particular term in that contract, parties will turn to metadata to help support their claims.

Another issue—it comes up with settlement issues. I'm involved in a case right now where we settled the case. We sent around the settlement agreement and the other side materially altered the settlement, causing the settlement to fall through, so we filed a motion to compel settlement, and now we're relying on these various versions of the document to support our motion. So metadata is increasingly becoming part of cases.

ROB KLEEGER: I would just say, for the years that I've been doing what I've been doing, it's in every case in one way, shape or form.

FERNANDO PINGUELO: This slide illustrates it well. Typically, in the old days, you'd get a paper document. That's what you see; an e-mail. But if you look at the metadata associated with the e-mail, you get to know [who] the author is, when it was created, when it was last saved, last printed, etc. This becomes important information if it becomes an issue whether or not a document needs to be authenticated or if the issue is when the document was created. Again, this is just a list—a variety of information—that is contained in metadata.

E-mail metadata is very important too. E-mail metadata is a little bit different than Word document or Excel spreadsheet data, but it does, again, give you information about the particular e-mail. Of particular interest [is] routing information on where an e-mail went before it wound up in the person's inbox. That sometimes gets implicated in cases.

The next hot topic is data protection and privacy. We talked a little bit about that earlier, so I don't want to re-emphasize that, but the point being that a variety of states—and I know you attendees are from all over the country—have certain data preservation protocols besides the federal rules and local rules related to e-discovery that may require notification of either employees or customers.

JULIENNE BRAMESCO: Fernando, we've got a very good question from the audience. What if a business receives

discovery requests or a subpoena for records that contain sensitive information? What does the employer do? What does a company do to protect that information?

FERNANDO PINGUELO: There's a variety of things that can be done and I'll show you an example that I'm involved in right now. The Department of Justice is conducting a massive investigation against a pharmaceutical company alleging health care fraud. Our client was just a simple vendor to this big company, so they were subpoenaed and brought into this criminal investigation simply because they did some work for them. We had a lot of issues related to lists and doctor information, etc., that we could not disclose. We worked very closely with the U.S. Attorney's Office to alert them to our concern, and through a combination of redacting and letting the source entity know what we were doing, we were able to produce the documents.

In that particular case, there's very little you can do when the government's involved and it involves criminal investigations, but what little you can do can go a long way in terms of protecting the information. The key is open discussions about the issue and addressing it right away.

Another hot topic, and the last hot topic, is the employee privacy rights. This gets into the issue of monitoring employee e-mails, etc. There was a case in New Jersey whereby an employee was communicating with her lawyer while employed, basically planning out a lawsuit of discrimination against the employer. What happened is: When the employee left employment, the company took her PC, had it imaged, and found these e-mails with her lawyer plotting about the lawsuit that she was going to file against the company. At the trial court level, the court held that that information, since she was on the company's system, on company time, was aware that the employer policy was in place, the court held that she waived her attorney-client privilege. The company was allowed to keep the e-mails that she had written to her attorney. That case was subsequently reversed on appeal, but the key lesson to be learned here—what saved the company—was having an amazing e-mail protocol that addressed the common issues related to the employee use of e-mail, but certainly made it clear that employees were not to use it inappropriately and it was monitored. The only thing that's worse than not having a policy at all is having a policy that is not adhered to. Fortunately for this company, they both had a policy and adhered to it very well, and that's what saved them.

JULIENNE BRAMESCO: I just want to point out that if you are a unionized employer, then you may have an obligation to bargain with your union over certain types of policies and surveillance.

FERNANDO PINGUELO: Correct. Finally just some pointers as I close my part of the presentation. You want to have policies in place that address privacy issues, employee issues, and e-data issues, and it's certainly something that we sit down, as outside counsel, with clients and experts like Rob and his firm to sort of map out what makes sense for the company. Because if you implement something that makes sense on paper and it doesn't really make sense when it's actually implemented, again, it's actually worse than not having a policy at all.

Cyber insurance protection: This is something Julienne had mentioned earlier and I thought it was a great topic to add here. Clients are asking, "How do I protect our business from data breaches?" So, there is what's called cyber insurance protection, where you can purchase insurance to protect against massive data breaches. There are a variety of products out there and it really depends on a variety of conditions and factors that need to be evaluated to determine premiums, but we're finding these types of insurance products out there and more and more readily available. The only problem is that they're very costly.

JULIENNE BRAMESCO: It's hard to underwrite when you don't know—it hasn't been done that much.

FERNANDO PINGUELO: Exactly, and I listed Marsh and Chubb as two examples. You can feel free to check out their Web sites for the types of policies they can offer. I thought it would be good to mention that.

JULIENNE BRAMESCO: I recently became aware of this new insurance product. And actually, if you get a hold of an application for the cyber insurance, actually going through the application itself is a really good tool for figuring out where

your liabilities are.

FERNANDO PINGUELO: That's a great point. That's what happens when you're securing this information. You go through a variety of checkpoints. They make sure you're in compliance. They make sure you have, as this slide indicates, a plan, and you stick to it. They actually force you to do what you should be doing on your own.

With that, Rob and I compiled a list of resources available to you. We tried to focus on government-sponsored resources to provide you with additional information related to e-data security in a variety of contexts that are listed here. This is some more information as well.

JULIENNE BRAMESCO: Just because I insisted that our members like to be able to look things up, so thanks for that. Thank you very much for a really interesting presentation. I do have a couple of questions. Before I get to those, I'd like to turn this back to Marni to give us the second verification code.

[*The CLE code and instructions provided here were for use only by attendees of the live webcast. To obtain your CLE certificate for this archived webcast when you have finished listening to it, click the EXIT COURSE button at the top right of the screen to return to your My Courses page and then click the certificate link or icon beneath the course listing. In the pop-up window, select the desired jurisdiction from the drop-down list and enter any requested data, such as your bar number and the CLE code that popped up while you were playing the archived webcast. (This code is required for New York and Ohio attorneys only.)*]

JULIENNE BRAMESCO: Thank you, Marni. OK, [we have] a couple of questions from the audience. There was a question about developing the work flow. This goes back to what I think is slide number 20, getting started with the basics. One of the points was to identify and/or develop a work flow to track how personal information is received and used. Do you have any advice on the best way to do that?

ROB KLEEGER: As far as from when I am approached in a situation, a lot of it is simply asking a tremendous amount of questions. What type of systems do they have? Do they have an exchange server, for one? This is talking to people that are involved, whether it's—you want to call it an audit on a proactive side. It's getting an idea as to what protocols and process are in place. How do people communicate with clients? How do people communicate with vendors? Is there any procedures that [are] in place? Are there any forms, that when you're setting up an outside party and they submit a W-9, if they're getting set up as a vendor or a new client in your system, what type of information do you capture? Once that information is captured, is it captured and stored locally on my hard drive or is it captured on a server somewhere? Is that server backed up? If so, where is it backed up and how often is it backed up? How often is it maintained?

I don't have a list that I would be able to necessarily send to anybody. It's really just going in and stepping away from what either your role is or, more importantly, pretend you know nothing about the business and get an idea in terms of how you do this. Once you do that, then what do you do, and where does it go from there? Those are the types of things that you can start to map out. OK, here's how this business operates or at least this is what I've gathered from speaking to multiple people. But you might find that not everybody's doing the same thing, which is a good problem in some respects to know, so that you can then put in a better procedure, and then train why they want to do it that way and the risks. And in some instances, you only want to provide information to certain people on a need-to-know basis. Not everybody needs to be e-mailed, "Here's a new client and here's their credit card authorization form." And believe me, I've seen all of that. And that's the problem, because if that one laptop that happens to be not protected by a very sophisticated password, and now all of a sudden anybody can go in there, look at those e-mails, and sure enough, they can look at all their attachments and see this whole entire file of credit card information at a single form.

JULIENNE BRAMESCO: Wow. I always felt sorry for that poor VA employee who took the work home and had his computer stolen and he was completely vilified in the press. I thought, "This poor guy's just trying to catch up on his work." So these things—it's real. It can really happen to anyone.

Do either of you have any thoughts about companies allowing people to use their own cell phones or iPhones for personal use? Are there pitfalls and dangers to this? I have an idea that we could probably spend an hour just on this topic. Any thoughts, though?

FERNANDO PINGUELO: I can pick up on that real briefly. We see it all the time because either the cell phone's issued by the company, or what happens more often than not, employees get their own cell phone and they're given a monthly stipend to cover the costs. The only thing I can say in either scenario is that just make sure you know the hardware, who's using what and when, and if it's company-issued, you'd better be sure that you have the inventory of all of the devices that are being used by your employees.

ROB KLEEGER: I actually had a conversation with a client yesterday about that very same topic. Again, to Fernando's point earlier, and it's been mentioned throughout, if you don't have a policy, or you do have a policy, you'd better enforce it. The reality is, just like Julienne was sending e-mails from her work to her home computer, which is something that everybody does, and everybody is a good person, is that problem that occurs when your laptop gets stolen and now you're the victim. That's the problem.

A cell phone is the same thing. Many times, organizations will be able to control their e-mails. Maybe they'll provide BlackBerrys that they'll give the employees; certain devices that are standard devices that the business can support. They can track that asset. They know what type of information can be controlled on that, so those e-mails that could very well be going through that BlackBerry server; they're in control of that. There's also technology out there and some things are pretty incredible. You actually have documents that can expire. You have information that you need certain keys and codes in order to view. In some instances, you can use those types of things, as well as, as technology continues to advance, and it's advancing at a far more superior rate than anybody's able to keep up with, but through the use of this type of technology, there's monitoring for cell phone devices. It'll always continue to get better and advance as we go along. Again, keep in mind how people communicate. By giving them 24/7 access, which is now an expectation that people have, that nobody is not available for 24 hours any longer. You're available because [clipped] to your hip happens to be a device.

JULIENNE BRAMESCO: Again, we could spend hours talking about the implications of the 24/7 workplace. Thank you so much, both of you. In just a moment I'm going to ask you if there are places where people can go about information about your firms or about these topics generally, but before I do, I just want to thank the sponsor, Meritas, again and to thank the audience for being here and for participating today, and also to remind everyone that ACC has a fantastic annual meeting scheduled for October 18 through 21st [2009] in Boston. There is still room available and hope to have as many of my in-house counsel colleagues as possible at the meeting.

I'm going to turn it back over to Rob and Fernando for the last word on how we can get more information.

FERNANDO PINGUELO: Rob and I have a variety of sources available to you and you can sign up for our newsletters. I run an educational e-data blog called *E-Lessons Learned*, and you can get newsletters [on a] sometimes weekly, if not monthly, basis on e-discovery and e-data best practices. Basically what we do is we pick apart cases, real-life examples, and identify what went wrong and what could have been done better in order to better educate businesses out there. We've set up the blog so that it is employee-specific, so we have low-level employees, we have management employees, we have in-house counsel employees, etc. So you could literally pick a category of employee and see examples of where employees did things that were inappropriate or negligent, and how it resulted in an adverse ruling on an employer, and how to learn from it. Also Rob does a monthly newsletter he can talk a little bit about.

ROB KLEEGER: The next slide will show our contact information, but I have an opt-out newsletter that I've been doing for several years which always gets a great amount of attention and feedback, where it really highlights a lot of the issues that are happening, not only electronic discovery, but just in the electronic world in and of itself. It's really done in a format that's like a postcard. It gives enough information that if you're interested, it gives you the sites to go and review that type of information that's of interest to you. There's some other helpful tips and whatnot, but you can send me an e-mail if you're interested and I can get you onto that monthly newsletter.

If you flip to the next slide, it'll have both our contact details for both myself and Fernando. Thanks very much for everybody's participation. Are there any other questions?

JULIENNE BRAMESCO: Marni?

MARNI CENTOR: It does not look like we have any more questions, so on behalf of the Association of Corporate Counsel and SmartPros Legal and Ethics, thank you again for listening to today's program.

[*The instructions provided here for obtaining CLE credit were for use only by attendees of the live webcast. To obtain your CLE certificate for this archived webcast, please see the instructions above.*]

Thank you again and have a good day.