ASSOCIATION OF CORPORATE COUNSEL

Protecting Individual Information--A Guide for In-house Counsel
September 6, 2007

Presented by ACC's New to In-house Committee, sponsored by Womble Carlyle Sandridge & Rice

Faculty: Michael W. Hubbard, Of Counsel, Womble Carlyle Sandridge & Rice; **Adam P. Palmer**, General Counsel & Chief Cyber Security Counsel, Cyveillance, Inc.

Moderator: Tim S. McClain, Of Counsel, Womble Carlyle Sandridge & Rice

(Tim McClain): Thank you, (Sandy). Good afternoon, ladies and gentlemen, and welcome to Protecting Individual Information, a Guide for In-House Counsel, today presented by ACC's new to in-house counsel committee and sponsored by (Womble, Carlisle, Sandridge & Rice). My name is (Tim McClain), and I'll be your moderator today.

Over 159 million data records of U.S. residents have been exposed due to breaches since January 2005. That's according to the Privacy Rights Clearing House. 159 million. If your company has not had a loss of personal information or data, it will. It's not a matter of if, but when.

A recent report found that 81 percent of companies responding to a survey reported that their organizations experienced one or more lost or missing laptop computers that contained sensitive or confidential business information in the previous 12-month period.

Another report found that one in 10 laptops were stolen, and 90 percent of those stolen laptops are never recovered.

Do you know how to respond to the loss of customer or employee personal data? An even better question is do you know whether your company has a privacy and security policy, and are you in compliance with the policy and all state and federal laws?

Today we are fortunate to have a very experienced panel of experts in this area prepared to address those issues and to answer your questions. Now, after the panelists have shared their ideas and experiences with you, we will open it up to questions. We understand this is an area of concern for many of you, and many have already submitted questions. If you would

like to submit a question, just go to the lower left hand corner of your screen, and there is a box there that will allow you to type in your question and then simply hit the send button.

Also, we'll be using a PowerPoint presentation this afternoon, which you'll see during the webcast. It'll also be available to you on the ACC web site.

There are also four items for you to download, and those are also in the lower left hand corner. These include a published article on the B&A privacy and security law reporter from August of 2007, and a privacy chart that you will be able to review after the webcast.

And it's also very important to ACC and to future webinars that you provide your feedback on this presentation. Please take the time at the conclusion of the broadcast to click on the evaluation tab on the web site and submit your comments on the webinar.

I would also like to point out the slide that is currently on, slide number four. Its entitled (Womble) Professional Privacy Consult. (Womble Carlisle) is offering participants in this webinar a free 30-minute consult with a privacy attorney, and you're invited to take advantage of that offer.

Today we have on the panel (Michael Hubbard), which practices in the Raleigh, North Carolina office of (Womble, Carlisle, Sandridge & Rice), and (Mike) leads the firm's privacy and data protection team. (Mike) co-authored the American Medical Association's Field Guide to (HIPPA) Implementation in 2002, and the AMA's (HIPPA) Policies and Procedures Desk Reference in 2003. (Mike's) article, "IPV6 Data Security and Privacy Concerns in the New Internet" will be published in the September issue of the Federal Lawyer in September 2007.

Good afternoon, (Mike).

(Michael Hubbard): Hello, everyone.

(Tim McClain): Also on the panel (Adam Palmer), the general counsel and chief cyber security counsel for the Washington, D.C. based cyber intelligence company, Cyveillance. Prior to joining Cyveillance, (Adam) served as the director of the office of legal counsel for the National Center for Missing and Exploited Children, where he focused on Internet crimes against children. (Adam) is currently the elected vice chair of the ACC's new to in-house counsel committee. Welcome to the panel, (Adam).

(Adam Palmer): Thank you, (Tim). It's a pleasure to be here.

(Tim McClain): And once again, everyone, I am (Tim McClain). I'm an attorney in (Womble Carlisle's) Washington, D.C. office. From 2001 to 2006, I served as the general counsel of the U.S. Department of Veterans Affairs. I was an integral member of the Crisis Management Team that handled the aftermath of the VA laptop loss in May 2006, which was the largest government data loss in history. I'll be talking about that incident a little bit later in the program.

Now, why should privacy and data protection matter to your company? How do you build or improve a privacy protection program in your company? And what is the role of in-house counsel in this endeavor?

To begin the discussion, I'll turn to (Mike Hubbard). (Mike)?

(Michael Hubbard): Thank you, (Tim), and we are very grateful to the ACC and to each of you for this opportunity to be with you today, and really commend the ACC on emphasizing this very important topic.

$256 million dollars. Let me repeat, $256 million dollars. That is the cost estimate by the TJX Company of what they've lost due to hacking of their information systems and the fraud committed by the bad guys with their customers' credit card information since around 2005.

According to the Boston Globe, one analyst believes that the figure could easily reach $500 million dollars, and perhaps go as high as $1 billion dollars. Obviously, there's very real quantifiable value to protecting sensitive information. In-house lawyers play a critical role in corporate privacy and data protection programs. You can really provide significant added value in designing, implementing and maintaining appropriate privacy and data protection programs, so let's roll up our sleeves and talk about the why, the what and the how.

First, why the privacy and data protection matters, second, what needs to be done to build an effective privacy and data protection program, and third, how can in-house counsel effectively work with other company stakeholders to make this happen.

So why do privacy and data protection matter? There are many reasons. Let's look at four key reasons. First, brand protection. Every company on this call cares about its brand. Whether your company has consumer customers or you're a B to B company with business customers, they expect you to protect their sensitive information, and your employees expect the same, and if you don't do that, you can face substantial adverse publicity, erosion of your brand and goodwill, and we've even seen a dip in stock price occasionally. Customers will walk away after a data breach.

According to a 2006 report from the Chief Marketing Officer counsel, it's called Securing the Trust of Your Brand, more than 25 percent of U.S. and European respondents indicated they would take their business elsewhere if a company compromised their personal information.

The second reason we care is legal compliance. We're all lawyers. Privacy is the law. You have a handout that you can reach during the login page for this webinar, and they include a list of selective laws and legal theories on privacy compliance to give you a flavor of how these issues pop up in different context. The actual specific laws that apply to your company depend on jurisdictional issues, where you do business, where you have customers, and what you actually do in your business.

There are some laws that apply pretty broadly. In the U.S., all companies face scrutiny under general consumer protection laws like FTC Act, section five. The FTC, Federal Trade

Commission, regularly enters into 20-year consent orders with companies that do not properly protect sensitive individual data.

(Adam Palmer): (Mike), this is (Adam). I don't want to interrupt, but just commenting for a second on your legal compliance point there. Or could you comment on the data notification laws that I think a lot of states are passing right now?

(Michael Hubbard): Yes. I think what I -- at least 35, perhaps now 36 state laws that the first one was California SV1386 that require in certain circumstances notification of effective -- affected individuals when their sensitive consumer information is exposed or lost, and obviously when you have to send out those letters with your letterhead and company brand on the letter, that can have a very serious impact on your brand and goodwill.

But you want to look at the FTC's web site; you'll see examples of those 20-year consent orders. Also keep in mind there are state consumer protection laws in addition to the data breach notice laws that (Adam) mentioned, and in some states like my home state of North Carolina, they can provide for trouble damages and attorney fees, and I think we're going to see more and more plaintiffs lawyers start to seize on that opportunity of using the consumer protection laws where privacy and security are compromised.

Third reason why privacy matters is compliance with contractual obligations. Pretty much every company signs non-disclosure agreements or NDAs or confidentiality agreements regarding information that the company receives from another company. Sometimes, and you've probably seen this in your experience, the confidentiality clause is carved out of any contractual liability (count), so although the value of a contract might be 10,000 or $100,000, the potential liability for breaching a confidentiality clause could exceed 1 million or even much more.

And fourth, getting privacy and information security right is the foundation for responsible information management. Let me explain what I mean by that, and if I had to emphasize one key point to take away from this session, it's to try your privacy program into other company goals and concerns. Don't just do privacy in a vacuum. The reason I say that is you'll do a better job if you take a holistic approach and you're more likely to get the resources that you need to do it right.

If you do privacy and security right, then what does that mean? It means you know what sensitive data you have, where it is, how you use it, which you share it with, and how you protect it. Privacy done well provides the necessary building blocks for other parts of responsible information management, which are protecting your trade secrets, mining valuable data, and responding to discovery.

Every company has trade secrets, whether it's Cola Cola, its secret formula, or any company for product generating customer lists, business methods, technologies, et cetera. An essential element in most jurisdictions of a claim for trade secret protection is that the claimant took reasonable steps to protect the information and keep it secret. Traditionally courts have decided what I call lock and key cases. What I mean by that is protecting trade secrets meant you had a paper list of who your customers are and you kept that list in a locked filing cabinet.

((Inaudible)) today in 2007 protecting your bits and bytes of data goes way beyond just locking paper in a filing cabinet. Let's look at a real world example that we've seen and you may have seen in your company.

A sales manager in your company leaves employment with a list of company customers and starts working for a competitor. You file your lawsuit; you seek an injunction to prevent the former employee and his or her new employer from using that customer list. If you do not have proper fire walls and access controls, you do not have an appropriate written security policy and documented training and so forth, and believe me, this is a list that can be a long list, then you should not be surprised if defense counsel challenges your claim of trade secret protection on the basis that you did not take reasonable steps overall to protect the information.

Another argument in the handouts that you have is a recent article in the VNA Privacy and Security Law Report that a couple of our partners here at (Womble Carlisle) on how trade secret protection and privacy controls intersect with each other.

Data is power. More companies are using data mining and so-called business intelligent software to better understand the marketplace and their own business. Here is how last week's Newsweek Magazine summed up the importance of data mining to companies today, and this is a quote I'm going to read to you from a book review of a book called Super Crunchers, and it's a book by ((inaudible)) and (econometrics) professor (Ian Ayers). Here's the quote; data mining is a microcosm of a powerful trend that will shape the economy for years to come. The replacement of expertise and intuition by objective database decision making made possible by a virtually inexhaustible supply of inexpensive information. Those who control and manipulate this data will be the masters of the new economic universe. I'll repeat that. Those who control and manipulate this data will be the masters of the new economic universe. Well, I think we all want to be masters of the new economic universe, and simply stated, data mining gives your company a distinct competitive advantage, but here's the rub.

To do data mining, you have to get to data, and you have to have the right to use it for the data mining purpose. Your use of individual customers' data is limited by privacy promises and privacy notices you provide to consumers regarding how their information will be used and disclosed, and it can also be limited by various walls and legal theories, and we particularly see this in the health care industry where (HIPPA) places restrictions on using and disclosing protected health information for marketing purposes.

If you have business customers, they're also not going to allow you to have their data and process it for your own data mining purposes. They don't have confidence that you have your act together and are properly protecting their data.

Well, we've almost come full circle on our responsible information management diagram. New discovery. If you've done the fundamental data flow mapping and data inventory for your privacy and information security purposes, you're in a much better position to know what relevant data you have when you need to institute a litigation hold or respond to discovery.

OK, we've discussed the why. Why privacy and security matters. Let's now discuss the what. What needs to be done?

An often overlooked but crucial aspect of establishing an effective privacy program that has well defined privacy governance in the organization. (Mike), what do you mean by that? Well, basically two things. First, who owns what controls, who's accountable for a policy or a procedure in a given environment, and second and critically, what is senior management's direction regarding implementing and managing this program?

The key next step is you need to identify and then classify what sensitive information you have. It's 220 here on the east coast. Do you know where your bits and bytes are?

Classified information is really getting important for this reason, not all information needs the same level of protection. The information about a possible merger or acquisition by your company may not need as much protection as information that a particular employee is enrolled in your medical plans.

(Tim McClain): (Mike), if I can interrupt for just a minute. I'd like to emphasize that particular point about knowing and classifying your information. I know that during the VA laptop loss, whenever we were trying to ascertain exactly what information was lost and what type of information was lost, we really ran into a lot of problems which made senior management decision making much more difficult than that, so it's very, very important to know what information you have and to know what classification that information is.

(Michael Hubbard): Thanks, (Tim).

Well, we've talked about what legal and contractual obligations you face regarding data protection. Also ask what are the industry best practices, the common body of knowledge of standards for information security that could apply to my company, say, under negligence standard, and then what specific regulations also apply depending on the nature of my business.

Many lawyers are surprised, and sometimes very surprised, at the breadth and the granularity of what are generally accepted security standards. There is a lot of documentation that's required, and we regularly help clients interpret those standards and then determine and critically document what they need to do to meet the standards. Once you've identified and classified your information and you've gotten a handle on the legal landscape, you need to perform a risk assessment. That basically means answering four questions. What are the threats to your information? Second, what vulnerabilities or weaknesses do you have related to those threats? Third, what would be the impact? What would be the pain point if data or systems are lost, stolen or compromised? And then, what would it could our company to better protect the information to get to a more acceptable risk posture? When you have answers to these four questions, you evaluate your existing policies, procedures and controls and update them to the appropriate level and detail for the risk tolerance of your company in this area.

Then, we all know this; you don't want to have a policy that just sits on the shelf. Sometimes that can do more harm than good. It's crucial to conduct privacy and security

awareness and training so, as some people like to say, the policies are baked into your company culture and values.

And the handouts that you can access from the web log in page, we cite one case where an employer was absolved of any liability for a data loss. And, that was because the employer had proper policies and procedures and had documentation that the employee involved had been trained on those policies and procedures. We also cite a case where an employee was vicariously liable because it didn't have proper written controls and training.

And then, always keep in mind that privacy and security are a process, not an end point. You need to periodically review and reassess where you are based on changing risks, changing threat environment, changing legal compliance standards and so forth.

We've talked about the why and the what. Let's now focus on how you, as in house counsel, can effectively work with other company stakeholders.

First, and always emphasize this point very strongly, make sure that the various stakeholders in your company understand the value of the attorney-client privilege and they're aware of your company's culture and approach to the role of legal counsel when the company performs risk assessments and does self-critical compliance evaluations. We helped many clients in getting in house counsel more directly involved – for example, with IT, when IT performs ongoing data security risk and compliance assessments. And, if you haven't gotten involved, I would highly recommend it. You will – you may be surprised of what kind of documentation is created, sometimes memos like the sky is falling, we absolutely have to purchase this control to protect ourselves. And, of course, that can be evidence in a courtroom.

When we do coordinate these activities with in-house client lawyers, we work together and we minimize the risk of security breaches that (Tim) will talk about. Help make policies operational and not just academic. And then, create and document legal defensible risk assessments. Second, you've got to get executive sponsorship. That's true for pretty much any initiative in a company. Preferably, somebody at the highest level practical needs to make two things crystal clear. One, what is the company's policy on protecting private and confidential data? And, two, everyone is accountable and needs to work together.

(Tim McClain): (Mike), this is (Tim).

Once again, just to emphasize executor sponsorship we found is absolutely critical. In the cases that we've handled, it's really a cultural change. In many of the companies, as you've stated, this culture has to be baked into the company and that's one assessment that I think everybody needs to make is exactly where is your culture regarding information security.

(Adam Palmer): I agree, (Tim), this is (Adam).

I just emphasize that point and that was a point I was going to make during my section of our presentation is that getting executive sponsorship is absolutely critical. Meeting with those executives and getting their buy in and backing for this. Because, you really do need to have ((inaudible)) big stick, I would call it, enforcement power to back up the program that you are implementing. It's an important program and it needs to be enforced.

(Michael Hubbard): Super, thank you guys.

Third step in how to get this done is to make sure you have the right stakeholders involved and, that they feel motivated and a real part of the process.

I'll take a moment and brag on a Fortune 250 company a (Womble Carlisle) client that did this very well. They started with a draft policy and they had individuals walking around to over 100 different stakeholders in the company for their review and comment over a nine-month period and actually did an accounting of what the comments were and how each particular comment was addressed in the final work product. It's basic human nature that people are more likely to buy into something if they think it's their idea or they had a part and a reasonable role in shaping a concept or a deliverable.

This slide includes a list of key stakeholders. HR definitely has a stake in this process. A lot of the data breaches that we read about are about your own – a company's own employee data. Name, address and social security number are the identify theft trifecta and every HR department has that information.

HR also wants to make sure that privacy policies are understandable and can be practically enforced. Some of the biggest risks are with third parties who have access to your information. And, this is where legal, I think, can be really helpful to procurement officials, contracts department, and doing things like preparing due diligence checklists for vendors. And, we've given you an example of one of those in the materials. And also, standard contract language that can be plugged into contracts as appropriate with third parties. I

In larger companies, corporate communications can really be one of your best friends. I've seen how they can really take policies ((inaudible)) draft and make them more readable. And also, put the information into an effective training program.

In summary, privacy and data protection are critical focus areas of any company. There is a logical progression of steps to put a company in a correct data protection posture and everyone on this call, as in-house counsel, can really be the glue that holds together a multi-stakeholder group to get the job done in a way that best serves your organization's mission.

At this point, we're going to segue way over to (Adam Palmer). (Adam) really has deep experience not only in handling these types of issues within his own company but also, in working with in-house counsel at some very large companies to help them manage their privacy and security risks. So (Adam), the floors yours.

(Adam Palmer): Thank you, (Mike). I thought that was great.

What I'm going to talk about with everyone is just of my perspective as one of your colleagues. I am the general counsel and chief cyber security counsel at Cyveillance Cyber Internet Security Company here in Washington, DC. And, both at my present company in that position and as the general counsel at my prior organization, I think it's very important with anything that you do – there's a lot of things that you can spend your time on. And, this is one of the big issues. And, I hope that if (Mike) didn't convince you, that I can

convince you in the next few minutes that this data protection really is an important issue for both the security of your company and the protection of your corporate name.

It's critical to good customer service. Not only complying with your non-disclosure agreements but, making sure that your customer's and your employee's data is kept confidentially. And – as I mentioned with (Mike), again I think he brought up a great point and this is true probably of any program and I may be, to some degree, pointing the obvious to you but, with any program that you implement, you need to have the authority to follow up on it and make sure that it's being enforced across your company, three months later, six months later and a year down the road. I think that if you do these things and you implement a data protection, data security program that you're going to avoid what I'm going to refer to as corporate chest pain down the road. I'm going to try to give you, here again, with this sort of rubber hits the road practical application of this, what I'm going to call, data protection in real life, the good, the bad and the ugly.

In my prior position – again, I worked for a very large non-profit that had connections with in-house who actually had several law enforcement agents assigned in-house. And, we dealt with some extremely sensitive information. Some of it was actually contraband that we dealt with on behalf of law enforcement and had Federal immunity to handle. But, it's some of the most sensitive information you can imagine that we had to secure. But, not only that but all the HR data and traditional types of confidential information that you might have to secure company. And, what you really need to have again, just to emphasize this, senior management backing. I've been fortunate that at every company I worked with – I've worked with other professionals, other executives who understood the importance and the scope of this critical need.

A motivated legal department. I was in charge of both companies and I was motivated. But it also really helps, in my third bullet point, on the data, to have a good IT department. I won't, I would have to emphasize here that it's very important not only to have a legal department that knows and understands this problem, but to have an IT department that's capable. Hopefully has some expertise in what types of data need to be secured and how it can be secured, but that can really work with you to secure it.

Let's look for a minute at the next slide I'm going to call the bad. At my prior organization, I did work with a chief financial, (net) financial officer. The CFO was a wonderful executive, very good at maintaining the books, but he felt that he had some very unique needs, I think as some executives do. And when I approached him about a data protection policy, he really was strong about that he had some special records and some special goals and he wanted some unique provisions put in for him.

And I think that that can be difficult at first blush, but sitting down with him privately, and I'd encourage you to meet executives like that half way, not only convincing him that I understood his needs, which I think he appreciated, but also helping him to understand that to the degree that I could, I would tailor the program, tailor our data security program to try to meet him halfway and understand and satisfy some of his concerns. And that really, I think, made him a little more flexible to meet me halfway. So do not underestimate the power of a little bit of flexibility and a personal touch.

I think the other thing that's bad, at least about approaching this problem initially as an in house counsel can be the overwhelming scope in finding resources, my last two bullet points on this slide. It can be a lot of information. And you really have to understand the scope of the issue up front. I spent a considerable amount of time, and one of the attorneys, the attorneys who worked for me spent a considerable amount of time at my prior company meeting with the various major department heads and understanding exactly what data was out there that we had to protect. And then again, finding the resources and committing our time to protecting them.

Let's move over to the next slide for a second. This is what I'm going to call the ugly of what I dealt with. The ugly is really the follow up compliance, and this can be probably one of the most difficult areas that you're going to deal with. Again, it's like anything, you can devote a lot of your time to it, but what happens six months or a year from now? We had a data or a document retention program at my prior company. It was, everybody knew what it was, but the question was, were people really following it? And that can be an issue with this also, and it's critical that you follow up and have that executive support and the buy in from the department heads to enforce this down to the lowest employee.

Look at the next bullet point there. I'm going to – this is something I really want to emphasize for a second, the why should I care. In my current position, I frequently meet with in house counsel at major corporations, and they often don't understand the scope of data security. How many companies spend a lot of money when you open a new office or open a new sales store somewhere and you spend a lot of money on physical security? You maybe pay for security guards out front in the parking lot, but then maybe don't spend a single dime or very little on actual data protection. And I assure you that those security guards in your parking lot are going to do little or nothing to protect against the loss of digital data over the Internet, your trade secrets over the Internet or the loss of a laptop by one of your employees.

Many, I've dealt with companies before who – for instance a pharmaceutical company where one of their scientists was blogging about trade secrets and/or putting information out that he thought just was simply being a good scientist and the scientific method, sharing information. This information was not found out by the company. It wasn't detectable under, with their commercial search engines, if they were just simply looking at Google. And they really didn't understand, and the employee didn't understand the importance of the data that he was sharing. And he thought he was just engaging in scientific discourse when really the company's view was he might be disclosing trade secrets to individuals who might not have the best interest of their company in mind.

So when you're considering data, don't just consider the physical data, the loss of a laptop, but consider all the information. The employee, the employee's children who may be listening and blogging about it on their internet pages, e-mail, the neighbor who overhears something and posts it on his Web site, maybe the third party who overheard one of your executives and posts something on an internet site. Your blogging policy is going to do little or nothing about that. And it's something you have to be careful of. Examine your entire Internet footprint and making sure that all the digital data within your company is protected.

Male: Hey (Adam)?

(Adam): Yes.

Male: I would just interject there that this really is a compliance mapping exercise. Information security, of course, was not invented from (whole clause). There are internationally recognized standards for how it's done. And I think this is really an area where legal can add synergistic value by working with information security managers and your company and learning more about what these standards are, where the cost benefit analysis is and addressing various controls and making sure that you've got them documented correctly. That's going to help you minimize loss, and then when loss does occur, you're going to be in a much better legally defensive posture by having had legal involved on the ground floor of that.

(Adam): And (Tim), or I'm sorry, (Mike) rather. I think that's a great point, and actually something I want to say. Now when you're trying to get that executive buy in and help them to understand the importance of this, you know, don't be afraid sometimes to point out to them that unfortunately there are some negative examples that you can use to show them on a practical level what they don't want to see happen to their company that has happened to some others that maybe didn't take this as seriously as they should have. So I think that using some of those examples and getting that executive buy in can be really powerful, and it's critical to success.

So again, the last slide here, what to do. Going forward, this is what I'd recommend based on my experience, again, working with other executives in my prior position. Understand the scope of the problem that you have, the types of data, how easy it can be to escape, examine and understand your entire internet footprint, all the data that's out there on this vast wild, wild west of the internet.

You must have the enforcement power that you get through your executive buy in. Tie this in with your compliance and security program. This is just as important as those security guards you're putting in the parking lot. And you need to be the leader. Don't set back and wait for the head of your IT department to take the lead in implementing an effective data security program.

Continually monitor to make sure it's compliant with what you've sets forth six months, a year from after it's been in place.

And if you're dealing with executive support, again, using some of the examples that I discussed, and sometimes collectively though working with other departments. I've seen great success, and I personally had great success in cooperating, using both the legal budget, the IT budget, maybe corporate securities budget to come up with the funds that I needed to implement a program that was going to successfully protect my organization and security.

And with that, I'm going to turn this over to (Tim) with his expertise and be able to tell you some real world examples that he has learned in his experience as a general counsel also.

(Tim McClain): Thank you (Adam). That's certainly excellent real world advice.

Ladies and gentlemen, I now want to have you think how you would respond to your worst nightmare. You get a call at 1:00 AM that the personal information of 26 and a half million of your most valued customers has been lost, stolen or exposed to public disclosure. What do you do? Let's talk a little bit about the (VA) laptop loss incident of May 2006.

First, what I want to tell you is that everything I'm about to say is public information. This is not attorney client privileged. It has come out in various reports, including inspector general reports and congressional records.

What happened and what did not happen? Why did it happen? How was the breach handled and what was the response? Whether you are a public company or a private company or even a government agency, the facts and lessons from this (VA) incident are important. What happened at (VA) could happen at any company.

Well what did happen? Let's take a look at it. First of all, very, very briefly, a (VA) employee took a huge amount of personal data home on CDs and DVDs. And then he loaded all of that onto an external hard drive. Sometime later, the employee's house was burglarized and a laptop computer and an external hard drive were stolen.

Well what did not happen? First of all, the laptop was not a (VA) laptop. It was a personal laptop. Second, there was no data on the laptop. Actually all the data was on the hard drive. And there was no breaches of data, as we found out later, the hard drive was recovered and the FBI forensics determined that the data had not been accessed. So there was no ID theft as a result of this loss. Yet, the (VA) loss is still the media tagline on every story about data loss.

(Mike) mentioned damage to the brand. That is the same for (VA) as with any company. (VA) is a brand, and so consequently the brand was tarnished as a result of this particular incident.

Let's go on to slide 20, as to why did it happen. Well the cause, and if you'll read the VA inspector general's report found that the main cause was a lack of a written and enforceable information security plan. VA has 230,000 employees. And normally, there are about 195,000 desktop computers and over 30,000 laptops. There was a great lack of awareness of any policy and lack of employee training on the policy within the department.

(Michael Hubbard): (Jim), I know you're going to speak to – this is (Mike Hubbard). I know you're going to speak to the data breach notice letter that you guys had to send out, but I just wanted to point out that good has occurred from this incident involving the VA. I had a client that had middle management that was really trying to push senior management into applying the resources to do privacy and data protection right and the company weren't getting along as far as they wanted. And then low and behold, the letters went out and the CEO and the COO of this client are veterans. They saw the letter, and they got the immediate impact of your company name here on the letter, and they realized in their retail company, they didn't want to be in a position to send those letters out. So I really appreciate your showing this to us because it does have the ability to effect management decisions in this area.

(Jim): Thanks, (Mike). And it's certainly good to hear that something good came out of the VA laptop loss. How about – how was the breech handled or the effect? The effect was essentially crisis management. In the case of VA is was an ad hoc crisis response teaming because there were no policies or plans for crisis communication or crisis response that were in the department. Obviously, today there are, and a good question for your company would be, do you have those policies in place? And of course, there was the national exposure and embarrassment that goes along with any of this type of exposure of a major company or agency.

There's actually a good study that is just out from the Harvard Business Review and it's on their Web site. It's entitled boss, I think someone stole our customer data, and it's actually a thought provoking case study with differing opinions on what you should consider and how you should handle a case like this, and I'd recommend that.

On to slide 21, we're talking about the Congressional response. Well of course the Congressional response started with a lot of hearings as it does in many times here in Washington. And so there were quite a few hearings, and in fact, they are still holding hearings because VA experienced at least two other significant losses, one in January of this year, and another in May of this year. And so they are still trying to determine exactly what occurred.

Also, there has been quite a bit of legislation that has been introduced in this particular area. They are listed in the slide for you. These are all senate bills. The first one is the Leahy Inspector bill was introduced in February and actually was reported out of committee in May. And it requires – one of the provisions requires every business entity that maintains data on 10,000 or more U.S. persons, shall implement a comprehensive personal data privacy and security program that includes administrative, technical and physical safeguards. And the program shall include a risk assessment. It also provides there should be notice without unreasonable delay. And unlike most of the other bills that are up there, this particular Specter-Leahy bill has a criminal provision in it, that anyone who knowingly and intentionally conceals the fact of a security breach and that breach causes injury to one or more persons shall be fined under this title and imprisoned for not more than five years or both. Now, once again, these laws are simply – in the case of S-495 it's actually sitting on the Senate floor, the other ones are still in committee being debated, but they are very, very significant provisions.

The one introduced by Senator Feinstein, S-239 is essentially the same as S-493. S-1178 is Senators Inouye and Stevens was introduced in April of this year, and it actually goes a different route. It requires a report to the Federal Trade Commission prior to any consumer notification and specifically preempts state laws on breach notification.

It also requires notification within 25 days, and requires notification if the breach "creates a reasonable risk of identity theft." It also gives consumers the right to place a security freeze on their credit report and in that case does not preempt state laws on freezes – credit freezes.

The last one is S-1260 was introduced in May. It does, once again, specifically preempt state laws, and it requires a notice when there is a breach that is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumer.

Let's go on to the next slide. Lessons learned from the trenches. I'll tell you, everyone on this Webinar, I wish I had had the opportunity to participate in a seminar or a Webinar like this one, 18 months or maybe even 12 months prior to the VA laptop loss, it may have been different.

The first issue is prevention. There's been a lot of discussion here about plans and culture and what you should do in your company. Can you prevent a data loss in your company? I'm not sure that that's possible. As I said, at the very beginning. It's not really a question of if; it's a matter of when. There is a lot of human element involved in this, and humans will make mistakes, and they will take data and put data on the Web that they should not have done. And so, consequently you need to plan and you need to do something up front. You need to be proactive. And otherwise, I guess, we'll refer back to Clint Eastwood, which was (Adam's) the good, the bad and the ugly slides, and his famous Harry line, "do you feel lucky?" And if you do, then you're fooling yourself. You need to develop and implement an information security plan. You need to have education and training of your employees. You need to become familiar with federal and state requirements. And you need to change the culture of your company to ensure that safeguarding personal information is the same as safeguarding national security information.

And how will you do that? You are going to do it through planning and preparation. You are going to plan for the crisis that will happen, not for the one that has happened. And you are going to raise the awareness. In this case, you are not just an advisor in your company; you are a leader in information security in your company.

If you take these lessons to heart and raise the questions that we've discussed you may not be able to prevent every potential data breach, but you will be in a much better position to respond to any breach and to protect your customer's interest.

Once again, I'd like to refer to slide 24 and it's entitled the (Womble) Professional Privacy Consult. (Womble Carlisle) is offering free of charge, a 30 minute telephone consult with (Womble Carlisle) privacy attorney. The number is on the slide. Please ask for Ms. (Kira Stelly). I mean we are a law firm so we have to do a preliminary conflicts check and we will do that, and then you'll receive a return call to schedule that – your participation consult.

That completes our prepared remarks. And what I want to do is open it up to the panel. We have received some questions, thank you very much. We're going to try to get to as many of those questions as we possibly can. And we're going to ask, (Mike); I think you've got a question that came in.

(Michael Hubbard): Yes, I've got several questions. I'll take the easiest one first. What is the FTC Web site referenced? It's www.ftc.gov. And if you click on privacy on that site there's really a wealth of helpful information as well as those consent orders that I mentioned.

I've got a question here, can inside counsel be held accountable for breaches? I would say if it's your laptop and you leave it in an unlocked car, there's going to be some potentially accountability within the company. From a legal standpoint, I'm not aware, yet, that any inside lawyer has been held libel in connection with a third party claim as a result of a data breach at a company. There have been, particularly in IT and other departments, personnel

changes as a result of how we publicize data breaches. I've never seen that hit a legal department.

I should say that we have seen class action lawsuits and derivative lawsuits as a result of some very highly publicized breaches. There's certainly management and the board need to be aware of responsibility in this arena.

And then if I can, I'll just address one other question, we have implemented some of the (statue) of ((inaudible)). How do we know if it's enough? That's a good question. From a practical standpoint, you ((inaudible)) reach a ((inaudible)) analysis, but at some point, the ((inaudible)), it's impossible to completely protect all data.

But certainly, you can make a determination that ((inaudible)) is legally defensible in the (faith) of any regulatory or third -- enforcement of third-party claims. And then it might involve -- it involves mapping what you've done to legal compliance standards and mapping what you've done to the general common body of knowledge of information, security standards that (Adam) and I have referred to.

What you'll find is you get into a functional status where you have your controls in place, then to achieve assurance as to those controls, you can prepare for an internal audit and have an internal audit, but also if the ((inaudible)) is ((inaudible)) and other areas that you can do a self-assessment on to reach a level of insurance that the controllers that you do have in place are being complied with.

(Adam Palmer): This is (Adam). I'm going to add one -- respond to one question that also came in, in the last few minutes. And the question is, how realistic is it that we will have a security breach at our company? And my response to that is again to sort of echo what (Tim) said in closing his presentation, which is do you feel lucky?

And I'll also say that there is probably a 100 percent chance that in some form, you will have some form of a security breach or loss of information, even a ((inaudible)) laptop information loss or a flash drive that somebody keeps on a keychain that gets lost.

But more than likely, and I -- just about every major company that I have worked with as part of ((inaudible)), we find that all of our major companies, you know, (again), (have issues of) maybe just an employee leaking some form of information or at some ((inaudible)) or some form of information that they may want to secure is leaking out across the Internet.

And again, the Internet can be a ((inaudible)) of information and it's very -- it's very important that you as a company and you as a corporate counsel take it seriously that -- and be prepared for when you do have that major threat that you've taken every step to hopefully prevent that from ever occurring and be prepared if it does ((inaudible)).

And that unlikely again, even if you've taken the steps ((inaudible)), that you know how to respond to it effectively.

(Tim McClain): This is (Tim). (Mike), I'm going to just add one other thing to the question or who asked about could an in-house counsel be held liable and I certainly agree.

Right now, under the current law, I've never heard of that occurring, but once again, I'd just like to go back to S495, which is the (Leahy Spector) Bill which is currently on the Senate floor, that it does provide for a criminal liability for anyone who conceals a data breach and there is harm due to one or more persons as a result of that data breach.

So in other words, the general counsel or someone else in the company if that becomes law, then there is the possibility of personal liability or criminal liability. We have several questions that have come in and I'm going to kind of group them together.

And I hope to throw this one out to the panel, is to what information security issues does a manufacturing company need to address?

(Michael Hubbard): This is (Mike Hubbard). I'll take a stab at that. Certainly ((inaudible)) we've talked about today, every manufacturing company has employees with sensitive data and manufacturing companies have clients whether it's a direct to consumer channel or business partners where you have confidential information you need to protect.

One of the things that I've learned with a particular client over the last six months or so is that there are unique issues to manufacturing in terms of process computing controls. It used to be historically, if you had just electronic devices on a manufacturing plant floor, they were standalone devices.

More and more now we're seeing networked systems and the same types of challenges to confidentiality and ((inaudible)) availability data by individuals can be the same type of challenges to a process computing control on a ((inaudible)) or ((inaudible)), a malicious hacker can shut down a manufacturing process through electronic means.

(Tim McClain): There is one other issue that came up and obviously the audience has quite a few in-house counsel in it and the question is a general question. Once again, I'll throw it out to the panel, is to how do I know when it is time for me to seek help from an outside source?

(Adam Palmer): (Tim), this is (Adam). Maybe all the in-house counsel now on the panel, I'll respond at it as somebody who is a general counsel and deals with hiring outside counsel. And my response in this regard that I think in this area that hiring outside counsel can be useful, especially in developing and validating your policies for data protection and understanding the scope of your issues.

In many of the cases that I've worked with, sometimes, you know, you may not have an IT department that can effectively deal with the issue or if you don't have a strong technical background, and let me emphasize that I had a pretty strong technical background and understanding these issues, so I was personally comfortable to some degree in going after this on my own when I implemented a program.

But if you don't have a pretty high level of understanding of these issues or a very strong IT department, that you may be placing your company in jeopardy by simply trying to go it alone.

And most of the in-house lawyers that I've worked with who have tried to create some type of internal solution or they use ((inaudible)) to find, you know, (threats) to their trade secrets

on line, I think that what they've found is that it is inadequate and they spent a lot of time when they have just spent a little bit of money up front and gotten some expertise from the beginning that it would have been worth its weight in gold.

(Michael Hubbard): Another ((inaudible)), I have had a couple of questions I'll try to direct quickly. This is (Mike Hubbard). Is there one location all the application privacy laws my company needs to comply with are located? Another way of (hitting) one location, and obviously, we have ((inaudible)) companies on the call.

But a couple of things I would point out domestically are the (FTC) Web site is a great resource. Your state attorney general may have some resources on the Web site. If you're in California, the California Office of Privacy Protection has some great materials and the National Counsel of State Legislatures has a pretty helpful site.

Keep in mind that those sites aren't always up to date and they're not always complete. This other question I have, should we screen our potential (hires) with these issues in mind? Absolutely.

If you look at some common information security standards like (ISO 17799), an international standard, one of the key -- one of the 10 key focus areas is actually personnel security and some of the biggest lawsuits we've seen in identity theft are insider identity thefts. It could be anybody in a call center.

Also, particularly where you have IT professionals who have administrative privileges, not just user privileges like (they all do), and ((inaudible)) especially an important place of trust and background screening is pretty much ((inaudible)) there.

(Tim McClain): All right, and (Mike), this is (Tim). I'm going to just take on last question here and it's regarding personal identifying information that you might give to a company contractor and how do you control that sort of thing?

And it's something that is a big concern because there is -- sometimes you can track for employee benefits or some sort of other benefit for the entire firm and so you're giving them personal information in order for them to provide the benefit. How do you control that?

You must provide in your contract clauses that lay out the standard for the security that you expect this company to provide to the personal information and what occurs if they do not. And indeed, I've even seen contracts with a liquidated damages clause in it and other damages information in it.

But these are great questions and we'd be remiss if we didn't thank you for the great questions.

In closing, I just want to say once again, we urge you to please use the evaluation tab on your Web site and please submit the evaluation of the webinar. Also we want to assure you that we will try and respond to all of the questions that have been submitted. We'll try and provide you with a written e-mail response either in the consult that we mentioned before or in writing. I want to thank (Adam Palmer) from Cyveillance and (Michael Hubbard) from

(Womble Carlisle). It has been our pleasure to do this webcast this afternoon and this now ends the webcast. Ladies and gentlemen, you may disconnect.

END