ASSOCIATION OF CORPORATE COUNSEL

Desktop Learning Webcast Transcript
Managing The Legal Risks Of Information Security... Be Prepared Or Face The Consequences!
June 13, 2007

Presented by ACC's Information Technology Law & Ecommerce Committee and sponsored by DLA Piper

Faculty:

Vincent Sanchez, DLA Piper Partner, and Co-Chair, Technology and Sourcing Practice Group
Karen Boudreau, Senior Legal Counsel, Websense, Inc.

Moderator:

Karen Boudrau, Senior Legal Counsel, Websense, Inc

Karen Boudreau: Welcome. I'm Karen Boudreau. I'm Senior Legal Counsel for Websense and I'll be moderating and speaking today. I first wanted to thank you for taking the time to listen to this Web cast. We hope you will find it informative and helpful. The IT and eCommerce Committee would like to thank DLA Piper for sponsoring the Web cast.

If you have any questions that you'd like to ask, there is a box on the lower left corner of your screen. Type in your question and hit the send button, and Vinnie and I will receive the question and we'll try to answer all our questions during the

Web cast. If for any reason that we don't get any of them, we will post the answers within about a week or so.

We also ask that you fill out your evaluation form, and the way you find that is in the box right above questions. It says Web cast evaluation. Please click on that and fill in and fill in the evaluation.

We're going to speak today about managing the legal risks of information security. You need to be prepared or face the consequences. I told you who I am. I'm presenting today with Vinnie Sanchez, who's a partner at DLA Piper.

He graduated from Notre Dame Law School and has his MBA from Northwestern. His practice focuses on complex technology transactions and life sciences and information services, sourcing, eBusiness, technology and information governance.

Vinnie is going to speak today about the business and legal implications of information security, particularly focusing on compliance and contracting. I'm going to talk about the kinds of technology available to help enforce policies and to protect information.

Vinnie, go ahead.

Vincent Sanchez: Thank you, Karen. I'm pleased to speak with all of you today. First I thought I'd start off with, you know, an overview of information security and why as in-house counsel and actually outside counsel, why do we care?

You know, first of all, it's a daily headline issue full of reputation and other risk, and if you haven't seen these types of headlines then you've been actually not reading the papers these days. But there's constantly something in the papers about information security.

With that, there's an increasing number of regulations and legislation that are being implemented and put before federal and state legislators to try and fix the apparent problems with information security and what is perceived to be a lack of security in many industries.

Information security generally is now a key component of really – and should be a key component of any compliance program. I'm going to talk a little bit more about that as we go through the program.

But anybody who's a public company and subject to Sarbanes-Oxley I think that's really sort of the first part of where people have been exposed to information security where you have to have accurate financial information.

And part of that is making sure that it's authentic, protected, not manipulated. And then if you're in other regulated industries, which I'll talk a little bit about in the next slide, you'll also have seen a lot of activity around compliance and information security area.

It's a key component today of most contracts where any information is exchanged. If you are responsible for contracts within your organization, you've probably seen a number of provisions around information security, around confidentiality that are not the ones we were used to just a few years ago.

Confidentiality provisions have been beefed up significantly and so have the allocation of the risk, which is one of the things I'll talk about during my part of the presentation.

And, you know, why do we care? Because to the extent that we advise senior management and boards of directors, it has become a significant issue for corporations. And surprisingly, a lot of people have been rather dismissive in some industries that are really not regulated, but even someone in the regulated industries about whether this is a board-level issue.

I will tell you from my perspective in working with other companies, it is clearly a board-level issue, and it's a question of at what level the board, you know, what committee of the board should be responsible for this.

And in some, you know, in some companies they've put it under the rubric of the audit committee because they've already been somewhat dealing with that in terms of Sarbanes-Oxley compliance. You know, I think that's one good place to start.

Some companies have started to think about whether they would have a separate committee that might be a technology and information governance committee that not only would govern the information security and information programs within the company but also the implementation of technologies not only to address compliance issues around information security but also just generally because as more and more businesses become reliant upon technology as an underpinning for their business and they become so reliant upon it, it may make sense to have a committee that sort of oversees that at the board level.

So that's some of the thinking out there, and I'll move onto the next slide. The – why do we continue to care? I mean if you look at some of the statistics, there's a new victim of information security identify theft every 4.5 seconds.

There have been, and this is maybe an outdated statistic because I think there's been more reported breaches since the first time I actually looked at the statistic.

But you know millions of Americans have been exposed to breaches. Hacking attempts continue, and the success rate continues to increase.

There's generally a lack of uniform security standards out there, which I think anybody who's been involved in negotiations or implementations of these types of programs is caused a lot of angst in how to deal with it.

There's generally from my experience in working with corporations trying to catch up and implement information security programs. There's generally a lack of sufficient corporate standards and policies generally, and a lot of companies find themselves behind.

And despite promises or representations that your marketing departments or other groups within your company may be making to the outside world, generally we find that information security programs within a company are not up to standards. And again, those standards are sort of in flux as well.

There continues to be a lot talk and news about vulnerability of the critical infrastructure of this country, in the federal government and, you know, generally around different types of software. And then back to the, sort of what I mentioned in the first slide, what you have out there is just an alphabet soup of regulations.

You've got HIPAA. You've GLB. You've got PIPEDA. You got, you know, FACT Act. It's just nauseating trying to figure out, OK, what's really the right standard for my program and how do I really implement this and pull it all together?

So when we look at why we – now we've looked at why we care, let's also talk a little bit about, just to set the framework for here are some of the things that are out there in terms of potential legal claims against companies that haven't implemented an information security program and haven't protected their information.

Obviously, a lot of people have heard about the FTC and state actions. There have been consent decrees under the theories of deceptive and unfair trade practices under Section Five of the Federal Trade Commission Act, similar deceptive practices under state laws and regulations.

And you know the FTC is really trying to stretch out its regulatory authority here in terms of trying to make companies do what they need to do to protect information. So they've really extended Section Five, particularly with respect to the unfair practices reach, to get into companies and make them do what they need to do.

And you know, one of the biggest claims out there was with Choice Point, and as many of you may know in January of ’06, Choice Point settled with the FTC that charged that it violated the FCRA, the Fair Credit Reporting Act and Deceptive and Unfair Trade Practice prongs of the Section Five.

And they paid about a $10 million fine, which was the largest civil penalty in FTC history, and they’ve, you know, expended a lot of internal costs just trying to fix the many problems that gave rise to the violations. And they’ve also had to settle with, you know, 44 states and also pay fines with respect to those.

So the potential exposure from that perspective is tremendous. Then you go into the part about, you know, what about claims against the company from the impacted victims of the breach, and that’s still really being worked out a lot in the courts.

You start to see some court decisions coming out, but there are tort claims, class actions that have been brought, you know, whether there’s a duty per state statute such as under California where you have a duty to implement information security programs under theories of fraud, negligent misrepresentations, unfair trade practices.

We’re starting to see a lot of different theories thrown out there. You know in a number of the cases, you know, some of them have been questioned as to whether there are actually any damages to support the negligence claim, so you've seen some cases thrown out by the courts, but they're – and in some cases there are damages to support the claims.

So they are moving forward through the courts. You generally had to have exposure to breach of contract claims to the extent that you obtained the information from another third party.

There's always the issue in question out there about whether your privacy policy has been positioned or could be construed to be a breach of – to be a contract and therefore give rise to a breach of contract claim.

And there's certainly some different approaches on how you deal with that and some of them are you know, incorporating the privacy terms within your standard website terms and conditions in order to attempt to try and limit liability. There are also some theories out there particularly around whether that would even be enforceable.

Based on choice ((inaudible)) and some other actions out there are shareholder derivative suits that you could be subject to for failing to implement an information security program that devalues the stock price of a company based on the potential breach and the negligence surrounding whether the company did everything it needed to do.

You also need to consider whether in your SEC filings, representations have been made around how you protect your assets, how you protect your information, especially for companies that have information as one of its main assets or its business is focused primarily around the sharing or selling or exchange of information.

So that's important to also look at and see that you're not misrepresenting anything in there and also that you're making the proper disclosures today about potential risk vis-à-vis the company in breaches and you know, how it might impact your business in the ever evolving changes around information security and the ability to you know, penetrate a company's information resources.

And then you know, in some cases depending on your industry you may find yourself afoul of and violating federal state licensure regulations and certifications so definitely a lot to be concerned about in this area.

So you know, when we look at a compliance program, what are we doing and what are we talking about? Well, first of all we have to ask ourselves what are we protecting? And today there's such a focus on the breach of consumer information or personal information personally identifiable information however you want to define that per different statutes.

But really, when you look at your information program, I tend to see a lot of companies focused only on that area because that's the one that's hitting the headlines, that's one where you're going to get in trouble vis-à-vis the FTC and other state regulations. And so that's the one that everybody is focused and concentrating on.

However, in your company, especially in this information age, it's hard to distinguish, I believe, from that type of information versus OK, I've got financial information which may or may not be subject to Sarbanes depending on whether you're a public or private company.

And I've got customer information, employee information, competitive business information that I obtain through well that's my own and it's proprietary trade secret information to my company.

Versus then again, third party information that I obtain through exchanges of that information pursuant to agreements I have with other partners, other companies, and service providers – just generally subject to non-disclosure agreements.

And so, when I work with companies, I really try to counsel them. We have to look comprehensively, ok, at all the types of information that a company is subject to.

We can't just say we're going to have this information security program for personally identifiable information and we're going to forget about all this other stuff because what you're going to end up doing is setting different standards, and you potentially give rise to claims against the company for breaches of this other type of information.

And again, you know, just think about contracts you have and that you're supposed to protect that information in accordance with standards on how you protect other information in your company and then can you really compartmentalize that and then subject yourself to the potential breach of that contract based on the fact that you've given different standards to securing that information.

So, again, really need to think comprehensively. And then looking at all this, always need to keep in mind – again, a lot of people are very focused on the digital world because that's where you see a lot of the breach exposure but you know, we've also seen tapes falling off trucks, tapes mishandled in the regular mail.

Just think about things in the physical world you know, and also file cabinets where information is collected, stored; just how people keep information on their desk. The program needs to really be all encompassing and look at all that.

In addition, it really needs to also encompass aspects of what could happen in a natural disaster. Had a situation that a company in Florida you know, through hurricane season their physical presence there, one of their stores was completely destroyed.

Yet, there were file cabinets left standing that had vital information of customers in it and you know, wasn't properly secured in light of the fact that there was a natural disaster. So companies are actually part of their business continuity programs need to look at that as well.

And that kind of leads into you know, the next slide here which is you know, looking at a comprehensive program. When you look at the legislation that's out there particularly GOB being sort of the poster child for how to really go about and attack compliance.

You know, your information security policy really needs to cover various aspects of how to deal with breaches of information. So, how do I respond to the breaches, how do I protect that information generally from a technical standpoint and also a physical standpoint.

How people within my organization are able to use information assets and resources. Do contractors have access to it? Who else might have access to it?

And then, what are the permissions around that and do I have written policies that I hand out to contractors that I attach to my contract about these types of things?

Going back to the aspect of making it a comprehensive program; record retention is also a key component of an information governance program. So I just don't want to focus on information security and looking at it from an information governance program.

So you need to rope in the aspects of record retention and how that fits in. How business continuity disaster recovery comes into this and then again, look at your employee handbook and figure out how all of this works under this general category of an information governance program; how do I manage information within my organization.

I've seen some programs set up that they don't really deal with record retention and how it works together with the overall program and the security of the information and you have sometimes have silos within organizations dealing with those two and you really can't have that because then the record retention as you may know, there are aspects of destruction of information and how you do that and you really need to pull that into, again, your information security program; how do I properly destroy that information so its not accessible to anyone else?

When we talk about the compliance program also, and implementing it, you know, we want to have some kind of information governance committee within the organization – and I would highly recommend that – and who's a part of that and that's always a big question.

Definitely want someone you know, the CIO or someone who's responsible for information security. Recommend ((inaudible)) representative from Finance and this again, goes under the notion that your information governance program is all encompassing including all the types of information that we just – that I previously just talked about.

Somebody from HR, somebody from Risk Management, possibly – depending on your organization – somebody from Contract or Vendor Management who has to deal with the contractual aspects of the exchanges of information, again, depending on your business.

And then business unit owners you know, but who do you invite, you don't want to make this committee so big, but I think you need to look at maybe, somebody from Marketing, somebody from Sales – depending again, on the nature of your business – but look at what makes most sense.

Who handles the type of information within your organization that may give rise to exposure and you want to have them as part of this committee in order for it to have buy-in. And also, to make sure that this – that your policies are implemented company-wide.

I've seen a tendency in some companies that I've worked with that the committee is organized of people that really are going to have a hard time getting buy-in within the organization and trying to implement this.

So you want to make it as far reaching as possible to make sure that everybody buys into this. And again, that goes back to senior management and the board. I think you have to get them to buy into why this is important and then once they get to buy in, it's a lot easier to implement a lot of the things that I've mentioned.

But you see in a lot of organizations – it's sort of like the world of the CIO and technology. For a long time, I think, and it may still be true in some organizations, senior management tended to be somewhat dismissive or didn't find it was important to have a technology person at the sea-level within an organization or have those issues brought to the board level, generally.

And now you see like the CIO's are a very important, critical component of the senior management. They report sometimes to the board, and different committees of the board.

And now I think that you're starting to see that in term of like, privacy, compliance, the privacy officer within an organization taking a higher roll and then that's why this committee needs to take a higher role within the organization because it's a part of compliance.

And you know, the last component of it is you know, having a person from Legal on the committee using that also as a way to potentially try and cloak in with you know, privilege around what's discussed at those meetings and some companies have separately a compliance function.

I wouldn't necessarily substitute the compliance function for the legal function because again, you want to try and cloak stuff in privilege to the extent you can. Part of the you know, your compliance program generally, the risk assessments and one comment on that is often we're asked as outside counsel to come in and do risk assessments.

I think there's two components to that; one is, there's a legal compliance part of it, you know, to say whether you have adequate standards in place, but part of it and a major part of it frankly, is really you need a technical person to come in to help you do that.

And someone who has you know implemented maybe a consultant who has implemented these types of programs before because there's so much from the practical, technical aspects that we just as lawyers are not going to be able to do.

What we do when we come in, as part of this is one, we look at your standards in place. We try to give you guidance on whether or not they comply with the sort of general standards that are out there that we're seeing.

But also we look at them frankly, from a pre-litigation or litigation viewpoint. I mean, are there things written in these policies 'cause frankly they're written primarily by technical people who have no aspect or appreciation for how this might play out in litigation.

So we try to look at saying, OK, are some of these statements in here going to potential cause us problems in litigation because some of them are very aspirational and we try to look at it from that perspective.

The other thing you should consider is going back to privilege, some of our clients have hired outside counsel in order to maintain privilege around risk assessments and then sometimes they put in structure where the legal counsel will hire the consultant to work for the legal counsel.

And that holds true whether the legal counsel is the internal counsel or whether it's the outside counsel in order to try and kind of maintain that privilege. And this is not something that I necessarily recommend doing ongoing.

I think in the initial stages, I think that's important because I think that's where you're going to find a lot of the issues and problems within an organization. You want to try and do the best you can to kind of cloak that in privilege.

As far as compliance program generally goes, I mean, part of it's doing due diligence any time you're going to exchange information with a third-parties. You know, what policies and procedures do you have in place to implement that diligence; whether you're going to send people into the field to do that.

This is also important with one of the later bullet points on overseeing service providers particularly around outsourcing. Do I have a program for diligence? Do I have a program for continuing monitoring assessments of my providers? Do I have a program for whether I'm going to implement that through questionnaires or on-site visits?

And a lot of this needs to flow down into your contractual provisions. Generally, whenever you outsource or have any service providers that are going to have access to critical information within the organization you have an incident response plan.

I mean, the first time you put together your plan is not when the breach occurs. You want to do that plan now. If you've been fortunate enough not to have a breach situation or potential exposure, do the plan now.

Run through some drills on how you're going to work this. I think it's the best thing you can do to be ready. Timeframes are short in terms of how you need to respond under certain state statutes. You really want to plug this into your governance committee function and maybe have a sub piece of that that's going to deal with these issues.

And then, how are you going to go about documenting. It's important, I believe, to document what you do in response to each incident response. You may make an analysis that you don't need to make a – to notify potential victims or people whose information may have been impacted.

Why did you come to that conclusion? Document it so you have that protection somewhere and that you've gone through a thorough analysis on that. I mean, if you look at what's happening out there; FTC and these regulations they're not saying that it's absolute in terms of your program.

They're saying that you need to implement reasonable measures to respond to incidents to have a reasonable program in terms of information security. OK, well, when those things happen, did you take reasonable steps to assess the risk, the exposure and that you responded to it and implemented measures necessary to do that.

I mentioned boards of directors before. Training is critical in terms of implementing the information security program. And then the last point on this piece is that on franchise systems.

If you are part of a franchise system or – the issues are a little bit different and I just raise it because technically, between the franchiser and a franchisee it's a third-party independent relationship but you're all operating under the same brand.

And I've had to counsel a lot of companies through how to implement an information security program through their franchise system because there are issues of how do you deal with breaches because independently even though you operate under the same brand, you probably independently have obligations to notify customers.

And this is a slight variation on what I'm going to talk about next which is how to deal with you know, contractual provisions around this. But that's an important distinction that people should pay close attention to if you're in that business.

So, going to the contracting approach, moving through this; approach is evolving on how to deal with this in contracts. You see people trying to implement reasonable standards versus strict liability. If you breach, if there's a breach while you're holding my information, you are completely responsible.

As opposed to, am I only responsible if I fail to implement reasonable standards and I was really subject more to a negligence type of action. So there's still that tension going on in terms of contract negotiations.

You know, again, this goes back also to scope of employment; did the person who breached or stole the information were they acting in the scope of their employment or is it the fact that they were merely my employee at the time of the breach whether they were acting in the scope of their employment or not and that we just merely had possession of it; am I responsible for that?

You have issues of companies wanting to test their outsourcing providers on you know, using detection or penetration testing and if you do that, what's the implications and liability around that?

Because if I want to test my outsource providers' systems by trying to conduct a penetration test and it takes down their entire systems, well, they're not going to be happy and they're going to want to be compensated and protected vis-à-vis their other customers. So that's been a big issue that's been coming up in a number of outsourcing contracts.

Incident response obligations. This is a situation – there's just a lot of tension right now because people just don't want to – don't know what to do and so it's a slight – I'm going to talk more on the context of third-party service providers.

Who notifies if there is a breach? OK, if the breach occurs at the third-party service provider, who is responsible, right? So, under state statutes some of the state statutes they – you as the owner and the data service provider who is processing the information may have independent obligations to notify.

So, how do you manage that? Because if it's my brand that's at risk as the data owner, I want to control that response and how it gets coordinated. And then what happens if there – we disagree?

That the service provider says that they have to disclose and we say no, we don't have to disclose what happens? Are there contractual provisions to provide indemnity around that? And that's not – you know, there's a question about whether indemnity even fully protects you because the service provider may be subject to federal or state action.

So, you really need to figure out how to coordinate all this contractually. It's got to be a coordinated response. And there's definitely a lot of tension around this and I have been working with companies where you know, the contractual provisions around this are now you know, two or three pages long.

Who's responsible for the remediation costs around potential breaches and again, going back to indemnification, how do you deal with continuing third-party losses? And you see a lot of legislation out there right now with banks being able to recover certain costs that they incur in connection with breaches of information.

So, that's also now going to start being built into a lot of contracts. And then you know, the last part about this is you know, have you as a company built in your contractual obligations into your overall incident response plan?

When you look at what's happening out there, people tend to focus on incident response plans as it relates to their breaches of information, but if you are a service provider and you have contractual obligations around incident response, vis-à-vis your customer or another third-party.

OK, have you tied those contractual provisions into your incident response plan? For example, you'll see in a lot of contracts it says, hey if you have my information and there's a breach, alright, I want you to notify me within 24 hours.

OK, well have you connected that to your incident response plan? Because when that governance committee or whatever committee you've established to respond to these incidents starts trying to figure out what happened and whose information has been exposed, I've seen in a lot of the instances where the last thing they think about is the contract, OK, and what they say about trying to notify people.

So, you need to have that factored in and it's somewhat a tedious task if you're a service provider but something that definitely needs to be factored in so that people can start looking at that right away and not find themselves in breach of contract.

So, with all that I know I've talked about a lot. Happy to answer questions at the end, but I'd like to turn this over to Karen.

Karen Boudreau: Thank you Vinnie. Could you move to my first slide please?

Karen Boudreau: OK. Now that Vinnie has got you all afraid, I'm going to talk about the technologies that can help to mitigate the risks. They fall into three categories. The traditional information security category; you're probably all familiar with that.

That's anti-virus software and firewalls and I'm sure your companies have that technology. There's also web-filtering which reviews the traffic leaving the network to determine if the destination is within policy.

For instance, the web-filtering companies identify phishing sites or other sites that can load bad information into a communication. For instance, if you put up the site it loads, it might load a key logger which will which allows the website to look at every keystroke that is made by that user and then what it does is it blocks the user from being able to access that website.

The last type of technology is a very new technology; you may or may not have ever heard of. It's called information leak protection and it focuses on reviewing the data within the network. What it can do is look at where different kinds of data are within the network like for instance, who actually has social security numbers on their PC.

So you can find out that there is somebody carrying around 40 million social security numbers on their laptop which could get stolen. It then manages where the information is transported.

You can set it to say for instance that social security numbers can only be downloaded by people in HR. And you can divide it by type of social security number; customer social security numbers can be downloaded by Finance, employee social security numbers can be downloaded by HR.

And then it can either report, quarantine or block information depending on the policies. So, information leak protection can say can send an email that says this person downloaded social security numbers and that would go to the compliance officer.

Or it can quarantine the download until it's approved, or it can just simply stop the download. It depends on what your companies wants to do. Let's look at the IT budgets. A very small amount of the IT budgets are being spent on security; about six to nine percent.

And then 40 percent of that is going to new technology so you can see it's sort of it's sort of like no more than two percent and the remainder goes to upgrade all the traditional solutions and that would be most commonly your firewalls and your anti-virus.

What we're suggesting is that you have an integrated approach to information security. If you look at this slide the kinds of things that can come in are spyware, Trojan horses, key logging, and then there's virus, there's a variety of web-based threats and then there's malicious code that can for instance wipe out your network.

We've all seen that. But there's also people coming that are inside the network, validly inside the network, who release information. And I think that's what we've been seeing with for instance the TJ Maxx case.

It can be done by employee error, it can be done by an employee who is simply trying to steal the information, it can be released by bad process. That's hopefully addressed by the compliance plan. And then of course there's always the angry employee.

The objective should be to create a safe and productive computing environment by protecting employees and the data for internal and external threats. The traditional security technologies are anti-virus, firewalls and then there are a couple that you probably haven't heard from heard of information intrusion detection systems and intrusion protection systems.

They look at the behavior of communication. Does it look like a communication going to a phishing site? And then it profiles them and blocks information that looks like it's going to a problematic site.

And security event management; that takes all the information you've gained from the anti-virus and the firewalls and the intrusion detection systems and puts it into a report so that you can analyze where the information is going.

Just so that you know about traditional technology, 98 percent of the companies have some yet 76 percent still have a problem. All these technologies more or less address an external site threat, not an internal threat. And many people aren't happy with the technologies alone. They're not really designed for the more complex information within sites.

Just as an example the State of Oregon Department of Revenue had to contact 2300 tax payers to notify them that their names, addresses and social security numbers had been stolen by a Trojan Horse program downloaded by a former employee who was surfing pornographic websites.

Obviously you need to have written policies that require ((inaudible)) enforcement those are the compliance policies that Vinnie talked about. You also need to look at the regulatory risk and the corporate governance issues and then of course there's personally identifiable data and the state ((inaudible)) laws that Vinnie discussed.

I'd like to talk about web-filtering. You might have experience with web-filtering at your company or you've experience it at some other company you've been at. The way it works is a screen pops up when you're trying to access certain websites and it can say a variety of different things.

It can say, you're using your quota time, you have a certain amount of time everyday that you can go to certain sites or it can block the communication entirely; it can say blocked by, in our case it says blocked by Websense.

These are very, very customizable programs. You can not choose to block, you can choose to just track where employees are going on the web, but you can also time access. This not only helps support employee productivity which was the original reason why many web-filtering programs were initiated.

But it helps block out unwanted code like key loggers, worms and Trojan horses, by preventing visits to the sites that carry that code. You can block by type of site, there are generally lots of categories. You can for instance, there can be pornography but there can be categories of pornography.

There can be hard-core pornography, there can be pornography like the Victoria's Secret catalog and then there can be art pornography, which would be certain photos and statues. It can also provide detailed records of all the internet activity. And it can also be customized to block by individual, or function, time of day, or category.

There are ten things I'd like to suggest that you might want to look at when you're looking at obtaining this technology. Clearly, it needs to be able to block web threats and you want to look at the best technology that meets both, how much you want to spend and what you need to protect your company.

It should anticipate, evolving threats. What you'd like to look for is a technology that doesn't just deal with yesterday's threats for instance; a virus that we know about but can look at something's a new virus that hasn't been identified yet – that's responsive to the web.

As you may or may not know the way phishing sites and key logger sites work is that they only stay up for a few hours and then they move on and get a new URL. So it's best to find a technology that continually searches the web and looks for those sites.

It needs to manage a number of different protocols. Problems can come in from a variety of protocols not simply one. And it should have a powerful policy framework, a variety of different categories, and different ways to customize the system.

It should also provide immediate notification or as quick as possible notification of problems. For instance, if there is a identified phishing site, hopefully, your technology will immediately send you an upgrade so that sot that it will be blocked if any employees try to access that site.

It should provide a lot of information to management so management can see how the web is being used by employees, whether or not we're having a problem with employees trying to go to sites or spending a substantial amount of time just surfing the web.

Obviously, it should be the best the best value for your money and hopefully it can manage all your exposure. Now let me talk a minute about information leak protection. As you can see there are a variety of different entities with confidential information.

R&D has probably your CAD files and your source code. Customer Service of course has information about your different customers. Legal as you know we have lots of confidential information about lawsuits, pending agreements, et cetera.

Human Resources has the background information for the employees, and Sales of course, has customer information. 80 to 90 percent of – actually, I'm sorry, 30 percent of all information leaks come from contractors which was why Vinnie was spent so much time discussing about making sure your outsourcing contracts deal with this.

And it's important to go visit to your outsourcers and see what they're doing. And interestingly you also have to focus on how these different constituencies share information. We may need to take some of the R&D information and give it to Sales.

Legal and HR as you know, share information on a regular basis. Information leak technology works by looking at data in a variety of ways on the network. Information leak technology can do an audit of all the data on your network by category that you choose.

It can tell you who has customer social security numbers, who has employee social security numbers, who has CAD drawings, who has source code. And you might be very surprised to see that you have a salesperson with the source code to your software.

And it allows you to go and delete that data if you choose, or at least know who has it. It can also monitor the data and see if it's coming in through – going out through the web through ftp files and it can also see what data is coming in that way.

It looks at the data being used, for instance, is it being used by it is being accessed by individuals in the company that shouldn't be accessing it. Do you have somebody from Sales looking at employees social security numbers for instance?

And it also looks at the data when it moves. It can look at data transmitted through IM, instant messaging, through internal mail, or through email, and it can also tell you when data is printed out. What we need to focus on is when you look at the products you need to make sure that it's accurate and that it includes all your proprietary data.

You don't want to get into a situation that you've missed some. It also needs to be able to enforce whatever your policies are by all kinds of data types, by ways of transmission in both for internal and external communications.

You should be able to update your policies. You can have it tied to type of data, to users, to regulations and you can have it automatically updated. And then you should be able to have to be able to manage your information and provide the reports that you need.

It's important to be able to know not only what's on your network, but what's happening to that data. So overall, you want to protect your data, you want to understand where your data is and where it's going and then you also want to make sure that you can that you can protect the data you choose to protect.

If you're looking to get products like these for – and I'm sure you already have the traditional products. Web-filtering, there are a variety of different vendors that sell web-filtering. Web-filtering is usually sold by subscription for terms of usually a year to three years.

And it's often sold by number of users so that if you have 500 users it's a certain price, if you have 10,000 users it's different. So don't expect to see a perpetual license for this type of software.

Because the databases are downloaded on a regular basis, the subscription is usually to the database of unacceptable URLs. Information leak protection is a very new technology. There are only a small number of vendors offering it at this point.

If you want to look at which sort of vendors you'd like to – that might work for you. The three leading vendors are Websense, Viracept and (Vontoo). And I think the Gartner there's a Gartner article that gives a very good summary of the different products and which might work for you.

The other thing you should know about both the web-filtering and the information leak protection products is they're virtually always offered with a free evaluation. You can load the product for usually 30 days and see how it works within your network and whether it's customizable the way you choose and how you want to customize it.

You can customize these to simply give you a report for both information leak protection and web-filtering. You can customize it to block certain communications and then you can also just have an email sent.

If you have any questions about the technology, feel free to contact me and I'll be happy to fill you in or get you any information you need. We had a few questions. The first one was – Vinnie, and you can talk to this more than I can – how banks are going after vendors for improper security measures.

I think there was a (TJX) has been presented with this problem. Can you go over what legal issues there presenting and kind of what you think about that?

Vincent Sanchez: Yes, sure. I mean this is actually the springboard for some current legislative activity and I think there's been at least one state that's implemented into law the ability for banks to be able to recover from merchants directly for these types of losses.

I mean, generally, you know, the PCI the payment card industry standard so anybody who processes credit cards is subject to these PCI security standards that are promulgated by the you know, Visa, MasterCard, and some of the other credit card issuers – or companies, sorry.

The you know, requires merchants and processors of credit card information to maintain a certain level of security with and have an information security program and what you've seen is some – Visa has actually fined a few companies for not being PCI compliant and the fines are fairly significant.

And so, I think the banks, prior to this legislation are trying to go in through the PCI standards in order to seek recovery against some of these merchants and I think we'll have to wait and see how frankly, some of that plays out because, you know, the banks don't necessarily all have direct contractual relationships with the merchants.

It really comes in through the credit card association such as Visa MasterCard and then again these PCI standards. But now that there's legislative activity around this, I mean, I think that's really going to be the hook for the banks to go after the merchants.

And it's also frankly, it's an incentive to get the merchants not only through compliance to the PCI standards, but also because they're now going to be potential other exposure. So really, everybody's just trying to put pressure on the industry generally, to – and what I mean by the industry, the merchants out there that are in non-regulated businesses.

Because right now when you only have GOB and HIPA you really only have those industries regulated so the banking industry and the – is much further ahead than any other industry and is used sort of again, as the poster child for how to do things right. And what you see now, and you've seen some of the FTC consent decrees.

They've extrapolated the GOB principles to non-GOB regulated companies apparently in some of their consent decrees. So, it's clear that that's the direction that they want you to head in. When you look at GOB – going back to one of my earlier comments around board of director responsibility – GOB does not specifically reference board of director responsibility.

However, there have been implementations of GOB between some of the like the banking regulators and SEC and some of their interagency guidelines specifically reference board of directors and if you take that as the standard for how everybody else should implement it, then that's why I keep harping on the fact that it's important to get the board involved.

So, hopefully that answers that question. I think, Karen, some of these other questions probably fall a little bit more into your area.

Karen Boudreau: Yes and so one of the questions was how do information security products handle portable devices that can take information off a system and copy and transport it wherever the downloader wants.

Information leak protection can be configured to prevent downloading off the network at all of certain kinds of information. It can prevent downloading off the network of certain types of information by any other group other than a certain type of employee.

It can further be configured to either track and or prevent downloading of whatever kinds of information you choose onto any portable device; a portable hard drive, a thumb drive. It can also not just prevent but it can send an email to for instance, the compliance officer to say, Karen Boudreau tried to download the source code for our major product or she did download it you know, kind of what do you want to do about that?

Further, it can quarantine the information. So, I would get a note if I was trying to do that that said that your information has been quarantined, it'll be released when and if it's authorized or it can say it's been quarantined contact the privacy officer.

So, it can either for that kind of information certainly, it can be blocked, it can – an email can be sent to a variety of different people. It can be sent to the manager, the privacy officer, the VP of Engineering, all three or it can be quarantined.

And Vinnie, we had a question about would you provide some sample clauses for outsourcing contracts which are favorable to the customer.

Karen Boudreau: Would you be able to post some of those?

Vincent Sanchez: Yes, let me see if I can look into some of those. Some of them have been very tailored to be specific to certain companies so let me see if I can give some general parameters there.

Karen Boudreau: OK, that would be great. And we'll try to post those when we post the answers to any of the other questions. Another question we had is what is the average number of resources required to maintain information leak protection products? It depends on how configurable you want your product and how often you want to change your policies.

Certainly, we're expecting that you won't need even one dedicated resource. You will probably need some implementation assistance, although you may be able to do it with a sophisticated IT department. But after that you should be able to have this be part of one person's job.

This should not have to be one whole person's job and certainly not more than one. But of course if you have a very large network, if you're General Electric, for instance, you may need more just by virtue of the size of the company.

Another question we had was how do I print or email this presentation. If you click on link number three in the links section, it says web slides, a new window will open and you'll have a PDF of the slides you can print.

And Vinnie, I wanted to ask you, where do you think the legislation is going and where do you think the courts are going to go in the area of information security? Do you think for instance, outsourcing vendors are going to are going to lose some cases or win some cases or do you think for instance the holders of the information like the companies will be held liable?

My understanding is that to replace a credit card, credit card companies want $50 a card. If you lose a million credit card numbers that could be a substantial amount of money. Where do you think it's all heading?

Vincent Sanchez: Well, that's a great question. On the legislative front, I fear that it's heading for an impractical disaster because if you look at what happened with the state notifications statutes, they really never had anybody who has to live with this in mind when they put it together.

To think that – or what the practical implications are, I mean to think that you're going to have the processor and the owner have two completely independent obligations to notify of a breach, it doesn't really help us you know, when we live in the world of the contracts and how the brand, you know, the owner with the reputational risk frankly, wants to try and manage that.

And a service – you know so you really have to place those two companies that are supposed to work together at odds. And so like any other legislation usually what happens in practice and I just I worry about what I see at the federal level, not really truly addressing that but what I do see is that we're going to have – companies are going to have to implement some reasonable standard reasonable standards and some kind of program in place.

I mean right now, the most of the statutes deal with just notifications but I think if they're going to take what California did and then impose an actual duty to implement security standards. I think people have been hoping that people would see with the FTC is doing and just let the industry take care of itself.

Having said that, when you look at what's happening in the courts, I mean it's still pretty early but I think the courts are going to definitely be very receptive to negligence claims and again that goes back to the duty to have to implement these security standards which are going to arise from either contracts or state statute or even deceptive you know unfair practices theories.

So I think that courts are going to be more open to that. Now the question on damages is always going to be an issue because what or the true damages out there. So I think that will be the biggest hang-up in the courts on that prong of a negligence claim.

In contracts, you're starting to see a lot of push-back. Traditionally, as you all may have experienced, if you had a breach of confidentiality provisions that are generally outside of any limitation of liability, for both consequential and direct damages, that's traditional that all how we started our practice.

I think you're going to start seeing a lot more push-back on that and confining that to you know, really a certain limited amount of information. I think you're starting to see vendors particularly tier one vendors like the IBM's of the world – and forgive me if there's anybody on the phone from IBM – but I think what you tend to see is that they're getting more sophisticated about this.

And even providers outside this country like in India are getting more sophisticated about it and not – they're trying to limit they're liability in breach of confidentiality which is difficult for any of us to swallow. ((inaudible)) kind of in the contract balance between general breaches of confidentiality and failure to implement reasonable standards to protect against that information from being disclosed.

And you know, that standard is becoming much more specifically articulated in contracts, but it's always been there I mean there's always been that standard you'll protect this information using measures not less protective than you would implement in your – with respect to your own information but no less than a reasonable standard.

I mean, so it's always been there, it's just that I think it's being recast and actually put with a lot more belts and suspenders around it and a lot more specific remedies around that. So that is going to continue to evolve as people try to deal with this and the continuing tension between you know having unlimited liability and having some limitation liability is going to continue I think. So, hopefully that answers your question.

Karen Boudreau: Yes, thanks Vinnie, and thank you and DLA Piper for sponsoring this Web cast. I want to thank you all for listening and of course, feel free to contact Vinnie or me if you have any questions. Also, we really encourage you to fill out the evaluation form; simply hit in the sort of center box hit the number one where it says Web cast evaluation and complete the evaluation.

The IT and eCommerce Committee will have a whole track of programs at the annual meeting in October in Chicago. We hope you all will be able to come and thank you again for taking your time to listen to the Web cast and you may now disconnect.

END