UIC John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 4 Article 6

Spring 2015

Legal Problems in Data Management: IT & Privacy at the Forefront: Developments In Cybersecurity Law and Best Practices, 31 J. Marshall J. Info. Tech. & Privacy L. 587 (2015)

SESSION FIVE:

DEVELOPMENTS IN CYBERSECURITY LAW AND BEST PRACTICES

MODERATOR:

MANUEL CUEVAS-TRISAN
VICE PRESIDENT, COUNSEL AND CHAIR OF GLOBAL PRIVACY AND INFORMATION SECURITY COMMITTEE, MOTOROLA SOLUTIONS, INC.
ADJUNCT PROFESSOR, THE JOHN MARSHALL LAW SCHOOL

PANELISTS:

BRUCE RADKE
SHAREHOLDER, CHAIR OF DATA PRIVACY AND INFORMATION MANAGEMENT PRACTICE, VEDDER PRICE PC

MIKE WATERS
SHAREHOLDER, VEDDER PRICE PC

PROFESSOR SORKIN: And our next panel will address developments in cybersecurity law and best practices. Our speakers are Bruce Radke and Mike Waters of Vedder Price.

MR. BRUCE RADKE: Good afternoon. Hi. My name is Bruce Radke. I am a shareholder at Vedder Price. I, with Mike, Mike Waters, my co-presenter, chair our Data Privacy and Information Management Practice Group.

Mike and I have had the privilege to handle numerous data breaches over the last several years, pretty much ranging to everything from sophisticated malware attacks to lost and stolen laptops to even the mundane where we had -- a health care system was transporting medical records to a third-party service provider, a storage site, the lid broke and blew open, and the records were spread all over. Those breaches have basically involved also sorts of stuff, basically from all industry verticals from health care, to financial services, to education, to manufacturing. Those breaches have ranged from two affected individuals to tens and tens of thousands of individuals.

If you have been watching the news you know that 2014 truly was a year of the data breach. What we have seen now with Anthem and some of the other breaches, 2015 is going to surpass that. So the bad news is and the lessons of those breaches are kind of twofold, both good and bad news. The bad news is this: data breaches are going to continue to happen, and they are going to continue to increase in terms of the number and the severity of those breaches.

But the good news is there are steps that you can and should be taking to minimize the risk of those data breaches and the harmful effect to your business.

So here's the agenda for the presentation, and we'll try to make up a little bit of time. We'll talk a little bit about the trends in data breaches that we have been seeing. Mike's going to talk about the enforcement actions, and I'll talk about some of the cases that have been filed as a result of the data breaches.

Mike's going to talk about, hey; we've had a breach, right? The question is not, are you going to have a breach, but the question is when. What do you do? What are your legal obligations with regard to notification following a data breach? Then we will talk about -- a little bit about the best practices in terms of data breach response.

We have kind of saved the best to the last. Probably the most important part of the presentation we left for Mike because he is by far a better speaker that I, much more engaging. He'll talk about what you can be doing now and should be doing now to minimize the risk of a data breach.

Let's talk about two trends. In the news you've heard about the

Target and the Home Depot credit card breaches. I think that's kind of top of mind of what folks have. If you may be one of the few businesses that don't transact business via credit card, you think, oh, maybe it doesn't affect us. But here are a couple of important statistics from the 2014 net diligence cyber claims study that looked at all the cyber claim breaches in 2014 and pulled out some interesting information.

I think the first one is, there are two points to this, Number one, PII, that is, name, first name, last name or first initial, last name and Social Security, driver's license, and account information that accounted for 41 percent of the breaches.

If you have employees, you have PII. You're at risk. What does that mean? The last part here is, if you look at all the costs of responding to a breach, I'm just talking about the cost of responding, separate and apart from any litigation costs or costs incurred in addressing a regulatory investigation. Just the cost of forensic investigation, the notification, PR, legal guidance, meeting costs is 110 grand. The average was 360 grand. Pretty high dollar amounts.

So, what are the hackers going after and how are they entering? They're doing it remotely. They're doing it by malware attacks and fishing attacks. What are they going after? They are going after credit card information. They are going after the PII.

The point to this slide is this, everyone is vulnerable. Recognizing how the hackers are going after our information, really I think the lesson learned there is, we've got to instruct our employees, particularly given the fact that a large portion of those hacks are social engineering.

We had a situation -- I may get an e-mail from Mike that says, hey, look at this Wall Street Journal article on the Target settlement. I click on the link and go to the Wall Street Journal site. But guess what, it's not the Wall Street Journal. It's a dummy site created by a hacker out in Vietnam so that when I click on it, it downloads some malware and goes into our system.

So training about the risk and how the hackers are accessing our network is critically important as we try to avoid those risks in the future.

A couple other things here --two other points. It's not Target; it's not Home Depot; it's not Anthem these hackers are going after. They're going after the low-hanging fruit. As those large organizations are hardening their systems the hackers are going after the low-hanging fruit, the small or the medium-sized business who may not be able to, one, have as high a safeguard to prevent those incidents from occurring; and, two, probably don't have as robust a monitoring systems so the hackers can sit in there and look at your business and do damage for a very long time.

Mike and I had an incident actually, we were just dealing with this morning, and I'll tell you, I got begrudging respect for these guys. It's

pretty amazing stuff that they do. We had a small eCommerce website, hosting site. Hackers got into their systems and spent six months, six months watching the business and watching how that business worked, what information was there, how they used that information. Then after six months they decided we knew enough and just started grabbing credit card information, volumes and volumes of credit card information.

The point here is 31 percent of the cyber-attacks occur at companies with fewer than 250 employees. Everybody's at risk. Again, the average cost of a breach is in excess of $300,000.

Here is the other critical part. Despite the fact that we're all at risk, only 77 percent of the small- to medium-size companies have cybersecurity plans or done employee training.

If you leave today with one thing, this is the thing you need to worry about. This is something you can do today as we leave. Mike.

MR. MIKE WATERS: Thanks, Bruce.

So I'm going to move into enforcement trends, and Bruce is going to talk a bit about litigation trends. Before I do so, let me give a brief overview of basically how privacy enforcement works in our country.

So we have what's called a sectoral approach. There are a number of countries, particularly countries in the EU that have agencies that are responsible for data privacy across all industry sectors or have a national data privacy law, and for better or for worse, we don't really have that.

We have the Department of Health and Human Services that oversees HIPAA and other health privacy laws. We have privacy laws that affect the financial industries and the telecom industries. We have federal agencies that are involved in privacy, and state agencies are involved in privacy. What that means is if your clients, your company suffer a data breach, the enforcement agency or agencies you may be dealing with is going to vary depending on what it is you do and where your customers are.

One thing that is, I guess, a fact of life, and perhaps a little bit frustrating, is, depending on what kind of breach you suffer and who's impacted, you may be dealing with multiple enforcement agencies at the same time.

So, for example, let's say you are a health care provider, and you're based in Illinois. You have patients from Illinois, Indiana, maybe some from Wisconsin, but then you also have patients who go down to Florida in the winters or Arizona in the winters; you have patients who are just in town and happen to get hurt, and you suffer a data breach and all your patient information is impacted. You will possibly be dealing with the state Attorney's General's offices of any or all of the states in which those patients reside.

In addition, because you're a health care provider, you will be dealing with the Department of Health and Human Services, their Office of Civil Rights as they conduct any investigation they may want to conduct. So you may be dealing with a number of enforcement agencies all at once.

So what are we seeing from those enforcement agencies? Well, first are fines. HHS actually happens to have some tiered civil monetary penalties. Other agencies enact penalties on more of an ad hoc basis. And there are really, as I see it, a number of things that I'm seeing.

One is a number of the agencies are very active at the moment. HHS is a perfect example of one. They're active, I think, in part -- and this is true with HHS -- in part because there are policies and procedures that they have mandated businesses within their industry have in place, and they realize that not everybody is actually doing what they're supposed to do.

So I can tell you from experience that we have a number of health care clients who have suffered data breaches and not all of them have the policies and procedures that they should have had in place pre-breach. I would say that most enforcement agencies recognize that even if you have the best security in place, you may suffer a breach.

The White House recently announced that Russia apparently had infiltrated the White House's computer systems. It happens. But where the enforcement agencies really get frustrated, where they really start to enact sanctions and fines is if they realize you didn't have the policies and procedures in place that we have mandated that you have. So the first thing we are seeing is that they are being very active, one, to fine people that don't have the proper policies and procedures in place; and, two, even if you -- I'll say that they're asking a lot of questions. Even if they don't issue sanctions or fines, they're asking questions.

So at this point in time, if you're in the health care industry and you suffer a data breach, maybe 50 of your patients, their personal information was disclosed. In the grand scheme of things, it doesn't seem very large. You will have an annual obligation to report that to the Department of Health and Human Services. Almost invariably, you are going to get a letter from them that is going to ask you a number of questions about that breach that you suffered. They will ask some things that may be easy to answer as to how did the breach occur, how many patients were affected, that sort of thing?

They will ask you about the security procedures that you had in place. They will go through your HIPAA requirements and ask you for copies of the policies and procedures that relate to policy that you should have in place. If you respond, sorry, we don't have that policy; we don't have that procedure, that's when you start to run into trouble.

So one of the trends I guess we're seeing is, mini audits, I would call it, from these enforcement agencies whenever you report a breach.

Another trend is, we are just not seeing fines, but we're seeing what we call kind of corrective action is being required.

These agencies, including HHS and the FTC, which we'll get to in a minute, will oftentimes fine people who have a breach, particularly when they think they didn't have the appropriate policies and procedures in place pre-breach. But they, then, are also required to take certain corrective action, which may be something as simple as, okay, draft those policies and procedures that you should have had. Oftentimes it's more complex. Oftentimes, there's an annual audit function that's involved, and you have to make annual reports back to HHS or back to the FTC over a period of 20 years. Sometimes you have to bring in an outside audit firm to actually do that for you, which can be quite time consuming and expensive. So that's another trend we're seeing.

This kind of goes to policy and procedure. But the other trend that we're seeing, really, is encryption. Everybody has been focused on encryption. It is one of the easiest things that you can do to protect your employees' information, your customers' information. If you lose that laptop and it's not encrypted, you can expect that an enforcement agency is going to give you a hard time, and that's true even if the breach is otherwise of no fault of your own.

So we have some examples here on the next couple slides of different unencrypted laptops that were lost or, in some cases, stolen, stolen out of somebody's car. You think to yourself, well, that's really not my fact, but if-- if the laptop was unencrypted, the enforcement agency doesn't care. They think, hey, listen, you should have had encryption in place and more than happy to fine you for that.

FTC, so if you're a health care company, for the most part Department of Health and Human Services is going to watch over you. There are some industries that maybe don't have a direct report, an enforcement agency that directly sees over them. So the FTC has kind of taken it upon themselves to sort of fill in the hole here, I think they view what they do as being incredibly important, in large part because oftentimes these large consumer class actions that arise out of privacy breaches don't really go anywhere.

Bruce can get into this in a minute, but the problem that plaintiffs' counsel had in those cases is that if there's a breach -- and you always get free credit monitoring from a company once you've had a breach -- if somebody provides you with free credit monitoring so you don't have to pay for that out of pocket, the courts have said you didn't suffer any damages, particularly if you didn't suffer identity theft; therefore, there are no damages. You have no standing. You can't bring this class action.

So the FTC has really decided to come in and oversee this issue. They recently entered into their 50th data security settlement. These oftentimes involve monetary fines. Again, oftentimes they involve corrective action plans.

In terms of trends, I think the FTC is big on a couple of things. One is: are you doing what you're telling consumers you're doing with their information? So, for example, we were talking about private policies just a moment ago on your website. If you're telling people that you do not share their personal information with third parties and a breach occurs, it turns out that it was, in fact, due to the fact that you were sharing personal information to third parties, that is something the FTC would very much be interested in.

State Attorney's General, so I was at a conference maybe seven or eight years ago and there was a representative from a state's Attorney's General Office who was asking a question from somebody in the audience, when do you really go after businesses? When do you fine them? When do you sanction them? And when do you just say, hey, breaches are part of life?

With all the qualifications that they always give that this is my opinion, this is not the opinion of the department, the answer at that point in time was, listen, at this point we're really just trying to work with you. If you have a dumpster out in back of your building in the ally and you dump a bunch of documents in there that contain personal information, yeah, we may fine you or sanction you in that situation, but otherwise, we understand breaches happen, and we really just want to work with you and educate you.

That is not the case anymore. Nowadays, a lot of state Attorney's General have become much more aggressive. In part, what I've heard from the agencies, it's because privacy breaches have become the topic on which people complain the most.

So, for example, Advocate over here had a breach not too long ago. I think the number I heard was the State Attorney's General Office received something like 40,000 complaints from people, and they're elected officials. People are complaining about it; they become interested.

As a result, maybe you're not in the health care industry, maybe HHS is not sending you letters after you suffer a breach, but when you have a breach, oftentimes you may be required to notify the Attorney General in the state in which the affected individuals reside, and many of those state Attorney Generals are now going to follow-up with questions. Sometimes it's in letter form. Sometimes you'll have to meet with them.

Our next-door neighborhood Indiana, if you have one affected individual that resides in Indiana, you have to let Indiana know, and they are going to send you a letter, in all likelihood, particularly if it takes more than 30 days in which to notify that person. So they have been very active.

On the slides here we show that they are issuing penalties.

Creative Health Care is kind of an example of this overlap. So at Creative Health, this is a situation involving an unencrypted laptop sto-

len out of a vehicle. They got hit by the Minnesota Attorney General's Office with a fine of $2.5 million, and the FTC also hit them. They had to enter into a corrective action plan in which they would be audited every two years over the course of 20 years. So oftentimes, again, you're dealing with multiple enforcement agencies.

PCI enforcement, so in addition to the state enforcement agencies, if you have a breach involving credit cards, you may have an obligation to basically pay fines resulting out of a lack of PCI compliance.

So I will turn it over to Bruce, and he'll talk about civil lawsuits.

MR. RADKE: So if you just had a breach, there is often a real rush to the courthouse to file a class action lawsuit. As Mike mentioned, in the absence of actual identity theft, those lawsuits have been dismissed for lack of standing, lack of any actual injuring fact.

So there have been a number of different theories that have been developed and will be developed throughout. The downside is, given the fact that there are so many breaches out there, the plaintiffs' attorneys have a number of different opportunities to test a lot of the new and unique theories. So everything runs from negligence to breach of contract, to failing to provide notification on time.

Before I move on, I want to point out one theory that I think is truly something we need to keep in mind; and, that is, fraud -- and Mike eluded to this -- misrepresentations made in your privacy and security policies. This is really a self-inflicted wound that you really don't have to sustain. Oftentimes what happens -- let me just ask you this, by a show of hands, who has refused or declined to engage in business with an online company based upon what they said in their privacy policy? Has anyone done that?

(There was a show of hands.)

MR. RADKE: Okay. A couple. All right. My guess is you probably haven't, right? But nevertheless, there are a number of different organizations that come up with very grandiose and very well-sounding, well-intended statements in their privacy policies that get them into trouble, and this is where the fraud claims come out.

When you leave today, go and take a look at what you're saying in your public facing statements online, your privacy policies, and your security policies. The next step, go and talk to the IT folks and say, hey, is this something that we actually do? Or do we need to make some adjustments in there in terms of what our representations are in our public facing policies? Or do we need to ramp up our security measures?

MR. WATER: So, for example, this is one that we see sometimes. Whoever writes the policy thinks maybe they'll find a copy of a policy

online that says, we use the most advanced security available in the marketplace to protect your information, right? They have a breach. Well, that's almost an impossible standard to live up to because things are always changing, and some customer says, listen, this was available; you weren't using it.

So that's where you really need to talk to the IT folks and figure out what you're doing and not just copy something that you found online.

MR. RADKE: So in those instances in which there has been no actual identity theft, there has been some very novel and creative theories that plaintiffs' counsels have come up with to try to get over that standing hurdle.

As Mike mentioned a lot of times whenever you get those letters, probably everyone has gotten the letters that offer free credit monitoring. That's not being done out of the kindness and goodness of the business who has sustained the breach. Yeah, it may be. But for large measure, it is done to eliminate the possibility that a consumer class action may be brought against your organization.

So in the absence of actual identity theft or you going out and buying credit monitoring services, there has been a couple different theories that's kind of percolated, and one was asserted in the RockYu case. There, there was, again, no evidence of any actual identity theft, and there, the plaintiffs' counsel said, there is a benefit of the bargain here. The PII that I gave you had some ascertainable value to you and to me, and that was compromised as a result or diminished as a result of the breach. That case -- that was sufficient to withstand a motion to dismiss.

Again -- so the courts have basically said -- and this is good news for us -- the mere threat that information may have been compromised without actual identity theft, in and of itself, is not sufficient. So the courts have dismissed quite a few data breach claims as a result of that.

But here's my take on this, looking in my crystal ball. Given the number of data breaches that are happening and the frequency that these are happening, we've got to win each one of these, kind of like the hackers, we've got to win a hundred percent of the time, and they just got to win once.

Same thing here, right? I think we're going to see more of the courts becoming more and more receptive to these cases as every day that the judges pick up the paper and see another breach.

So I think we're going to see some more novel theories. Again, here's the benefit-of-bargaining case that I talked about with RockYu.

Sony. This is a prime example of what Mike was talking about, about those representations that we make in our privacy policy. Taking a step back here and what got them into trouble was they said they used industry standard encryption. Doesn't seem too terrible, right? Not

too egregious. But that cost them -- that cost them about $1.5 million.

Same thing with LinkedIn, protected with industry protocols and technology. That one cost them $1.25 million.

Now, Target -- I'm losing track of time – the Target case settled, I think what, ten days ago, somewhere in there. A great settlement, right? It involved 42 million people with their credit card and debit cards compromised. Settled for 10 million bucks. Plaintiffs' attorneys made $6 million out of the deal, but to the class, $10 million. If you look at the other cases, like the Sony PlayStation case, it involved $31 million for 15 million users. The Target breach is a real good deal. Same thing with LinkedIn.

Here's kind of interesting. If you're in the health care field, one trend of settlement is, those cases or those settlements tend to be a little bit higher, as evidenced by the Stanford University Hospital settlement. There only 20,000 affected patients. Quite frankly, guys that is a very, very small breach, right? That one settled for 4.1 million. There are somewhat extraneous circumstances, but I think it demonstrates health care is a big one.

The other thing we're seeing was demonstrated in this AvMed case, and Mike talked a little bit about the OCR and FTC enforcement actions. Their settlement agreements, what we're seeing is not only monetary settlements but also different types of non-monetary terms that folks have to engage in a kind of corrective action plans, kind of on a private matter. I think we are going to see more and more of those on these kinds of settlements.

So with that said, let me turn it back to Mike but, before we do that, any questions so far? Yes, sir.

FROM THE FLOOR: With all the numbers that are out there that are really large, four settlements, or even for hypothetical cases that you go to trial and succeed, what kind of costs do businesses incur just to sort of swat away the dismissal? These cases are brought up and dismissed. There is still an attorney that you're paying to go to court to handle those, are there any sort of numbers that can be readily assigned just possibly dealing with that aspect of breaches?

MR. RADKE: Yes, as you can imagine, those costs are not insignificant, right? So the cost of defending and prevailing on a class action case is pretty significant, certainly tens of thousands or hundreds of thousands of dollars.

MR. MANUEL CUEVAS-TRISAN: A comment as well, there is also the element of remediation, right? Even if you win the case and you have to pay for -- counsel knows how to pay to remediate, and sometimes we would even have to demonstrate that -- the plaintiff demon-

strated that you are liable. So there's a significant business cost associated with this.

MR. RADKE: Not to mention the fact of potential lost business and lost good will and lost reputation.

MR. WATERS: Yeah, and to your point, we have had couple recently involving some pretty bad malware situations where IT staff of the company is literally working 24/7 over the course of a month to try remediate the situation.

MR. CUEVAS-TRISAN: Oftentimes, you have to bring contractors in.

MR. WATERS: Absolutely, yeah.

FROM THE FLOOR: You mentioned that Attorney's General and the FTC and other regulatory agencies are requesting information concerning their policies and procedure that organizations have in place when they report a data breach and under various other circumstances. So, obviously, having a policy is great.

The other half of the battle is following the policy, and in order to follow the policy, at least from the standpoint of working with the regulatory agency, you have to show evidence that you are complying with the policy.

So my question for you guys is: In your experience, to what extent are you seeing things like privacy risk assessments, security audits, and privacy impact assessments being included in these requests? Is that something that's being privately sought by these regulators or is that something that isn't a trend at this time?

MR. RADKE: So my take on that is absolutely yes. We kind of know who the regulators are, typically what they ask for. If we've got a breach involving this particular jurisdiction, we generally know, all right, I know he or she is going to ask, one, two, three, four, and five, right? Over here, they are going to ask A, B and C.

To your question, if you've got a breach, for instance, like in Massachusetts, we know they are going to ask for written information security plan. We know they are going to ask for the incident response plan. What has been a trend is, what have you done in terms of protecting or taking precautionary, proactive measures? The risk assessment is something that -- I think we're going to see a lot more of.

Mike, thoughts on that?

MR. WATERS: Yeah. That's absolutely true. A couple things to

your point. So one is, in addition to asking for policies and procedures, they do oftentimes ask whether the policies and procedures were followed.

So, for example, we just did a response the other day to the Department of Health and Human Services. There was a laptop theft. The laptop was supposed to be kept in a locked secure location. One of the employees just simply forgot to lock it, and apparently somebody at night came and stole the laptop.

So as a health care organization, they were required to have a policy that relates to employee sanctioning, and the Department of Health and Human Services requested a copy of that policy and then asked for evidence that they actually followed that policy when dealing with that particular employee that failed to lock that room, basically. So we have to provide a copy of that employee's file, show what happened. So they are absolutely asking those questions.

The other thing, the risk assessment oftentimes helps in terms of shaping the narrative. So if you're having a discussion with an enforcement agency, you want to convince them that both pre- and post-breach you took the situation very seriously. If you can demonstrate that you conducted a risk assessment and acted upon whatever the findings that risk assessment bore, that definitely helps shape the narrative.

So you suffered a breach. What are you legal obligations in response? Maybe the easiest way to do this is -- we'll take a hypothetical company. Let's use what I was talking about earlier. We'll say a local health care provider. Most of your customers are from Illinois. Most of your patients are from Illinois. You do have patients from surrounding states. In addition, you have people who come for x-rays and have broken bones fixed or are in from out of town. You have those people who winter in Florida and Arizona. So you have patients from, we'll call it, 40 states around the country, and -- there's a malware incident. Somebody winds up having access to your patient database. What do you have to do?

Well, there's some non-legal things that you have to do -- immediately you have remediate the situation, stop the breach. Then in terms of notification, you do have legal obligations as well, and there has been a lot of talk over the past few years about enacting some sort of federal notification law. For whatever reasons, that keeps failing to get passed. As a result, we're basically operating under what is largely a state framework. So a company that suffered a breach, you have to look not just at the breach notification law in the state in which you're located, but the law in which the affected individuals reside.

So if you are a local health care provider but you have patients from 40 different states who have been impacted, you have to look at 40 different state breach notification laws. In addition, if you are in a regulated industry such as health care that has its own breach notification

law, you have to look to requirements of that law as well.

You may also have, if it involves credit card information, PCI requirements. We'll talk a little bit later about business associate agreements. But if you're a health care provider and you have somebody else's data as well, your agreement with that other company may require you to provide notification. It probably does require you to provide some sort of notification to that entity.

MR. RADKE: One other thing. We have been talking a lot about health care, because that's honestly the circumstances in which these breaches arise. But even if you're not in the health care field, you're not out of the woods.

We had an instance in which kind of a smaller business, who was fortunate enough to have customers basically all across 50 states, they got involved with a breach. Quite frankly, they had to deal with the notification statutes of all 47 states. So it's not just health care. It depending on the problem and the size and complexity of your business, it may be much more.

MR. WATER: Particularly now that we're in an online world with a lot of companies, perhaps most companies have an online presence. Many of you or many of our clients are going to have affected individuals who reside all over the country.

At this point, 47 states, D.C., and U.S. Territories have breach notification laws. Alabama, New Mexico, and South Dakota are the only exceptions. It looked like a couple weeks ago, New Mexico was going join the list, but that one ended up failing just last week in their legislature.

I am going to skip some of this in the interest of time, but there is definitely some common themes as it relates to all these breach notification laws. A definition of what's a breach is oftentimes pretty similar. So the most common definition of a breach is the unauthorized acquisition of computerized data -- some of the breach notification statutes don't apply to hard copy records -- that compromises the security and confidentiality or integrity of personal information. There are some alternative definitions, and we get to some examples of those here.

These breach notification statutes typically deal with PII or personal identification information, which is the individual's first name or first initial and last name in combination with one of these elements. Typically, these laws are concerned with, is this type of information that can lead to identity theft? But we have seen over the course of the last few years that some of the laws are becoming a bit more broad.

Biometric data, for example, has been added to a number of state breach notification statutes, even though that may not lead directly to identity theft.

So what you are going to do if you suffer a breach, basically work

with counsel. But you are going to examine whether you technically had a breach under each of these states, with federal agencies' breach notification statutes, and then you're going to look at things such as timing.

So many of the states have a specific time in which you have to notify affected individuals. It can range from basically 30 days to 60 days. Other states say you have to act within a reasonable amount of time, and you are left to yourself to figure out what reasonable means. But we have seen one of the cases that we had earlier; it was Kaiser Permanente in California. They got fined because it took them three months to provide notification, and California said that that was not reasonable.

You will have to take a look at not just timing. I'll take a step back. If you're in a situation where law enforcement is involved, like the hacking situations, malware situations, law enforcement may ask you to delay notification, and then you're allowed to do so basically in every jurisdiction.

Different states have different ways of the people you have to notify, but almost all require you to notify affected individuals. Some require you to notify credit agencies. Some require you to notify state Attorney Generals of their particular state. Some require you to do that if a certain number of individuals were affected. Some, such as Indiana, require you to do that even if one individual is affected.

Different states have different ways in which you're allowed to notify. Most allow for written notification, but if you have a very large breach, some allow for e-mail notification, public notification. Sometimes you have to notify the media.

So what you have to do, if you have individuals in 40 different states, take a look at who do we have to notify. It may be more than just sending out letters to the affected individuals. You may have to notify certain state AGs. You may have to notify the media in certain states and so on.

A number of the states -- most of the statutes talk about the content of the notification. You are supposed to include certain information in the notification that goes out to people.

So with that being said, Bruce will talk about best practices.

MR. RADKE: If you've had a breach here are some of the questions you are going to be asked. It's not just questions from regulators, its questions from your employees. These questions will be posed by your board, by your shareholders, by the media, by the affected individuals.

If you have a breach at your company, how can you answer these questions? Do you have a written information security plan? What's your incident response plan look like? What security measures did you have in place to prevent this breach in the first part? What have you done to address the breach?

Let me ask you, how comfortable would you feel if you have a breach now answering these questions right now? The reason why I bring this up, is knowing what's going to happen at the end and what you're going to be dealing with is a good way to decide how are we going to respond and what is the best practice for responding to a breach. Not only are you going to be dealing with a lot of questions, but you are going to deal with a lot of decisions. Right?

Breaches happen in realtime, it's a truly 24/7 proposition. You're dealing with crises, and you're dealing with a ton of moving parts. What you're trying to do is make sure that all the parts march in the same direction, and you have got a lot of decisions, and the decisions we make today, right now, here, will have cascading effects, or effects that won't be felt until six or eight steps down the road.

The point of all this is we need to think about these questions and how are we going to make these decisions before a breach happens.

You don't want to do it in the crisis, in the breach, literally in the breach of the breach, right? So a couple factors influencing the cost of a breach, and again, this also should drive how you respond.

Have you prepared for it? Do you have those right policies and procedures? Are you using the right outside counsel or outside investigators; the right forensic investigators? How quickly do you respond? Quite frankly, you need to proactively manage the breach rather than continue to react. The only way you are going to be able to do that and do that effectively is do the tabletop exercises and do mock breaches.

A couple things. Every breach has its own little unique quirks and turns. There's a couple themes that go throughout, and each one of them are not created equal. You are going to have to have a tiered approach.

So the lost or stolen laptop is handled a little differently than the malware attack that has infected all your systems. So your response plan has to take into account those different levels of severity and how you respond to each one of those appropriately.

Here's kind of a simplified view of the data breach, right? You discover a breach. You evaluate the breach. What's the scope and effect? Who does this affect? Managing that kind of short term, and then how are we going to handle it in the long term?

First thing, understand the scope. Who's been affected? How has it happened? It must be managed, not simply responded to.

Long story short is, you need a General Eisenhower. Or one of our shareholders, John Cleary out in New York always says who's your Eisenhower? You need somebody there who's going to direct the troops to make sure all the troops are marching in the same direction and all on the same page. Absolutely, positively critical to have somebody that has gone through the process before, because, again, I will tell you if you're dealing with law enforcement, you're dealing with the media, you're

dealing with board members, shareholders and all the other sources. If there are a lot of things going on, you need to make sure that everyone is marching on the same page. There needs to be one person to make sure all the parts are fitting together, moving together. It doesn't happen in a vacuum.

Mike and I had a breach early on. It happened to be a medical processor, medical billing processor, and they had a breach. What they had, a couple of their IT guys decided, hey, they could develop a better secret sauce, and so they went out, and they grabbed the secret sauce from our client but inadvertently grabbed a bunch of health information from a lot of their customers and took it.

The problem, not only was it a huge problem, but our client was in the process of being sold. I remember being on the call with the CEO and talking about, hey, do we have to notify several million people?

He said, look, we're in the process of getting sold, getting chopped. We do this, all the hard work that we hit, put into the last 25 years in developing this company, gone.

So you have got to understand that. Some are easy. Some of them are much less clear.

Here is another thing. As Mike said, things are going to happen. Deal with it. Be upright; be forthright with law enforcement, with the affected individuals, and with the regulators. It happens.

Then once you do have a breach, conduct a postmortem. What have we done? How could we have done it better? Then build that back into your plans.

Mike.

MR. WATERS: All right. So risk mitigation. We have a little statistic here. 87 percent of breaches could have been avoided through reasonable security controls. Sometimes breaches happen. Russia hacks the White House, but 87 percent of breaches could have been avoided through reasonable security controls. 60 percent is the percentage of incidents where policy was in place that would have prevented a breach, but it was not followed, and a breach occurred.

So you will probably give some thought to this. Maybe your company has a policy; don't e-mail confidential documents to your personal e-mail account. People do it all the time. They want to work on the weekends. It's the easiest way to do things.

Or, maybe it's something along the lines of -- something as simple as there is a waste basket in which we are going to throw away all documents that have personal information on it or all confidential documents. It turns out that a lot of people just aren't using those wastebaskets to throw those documents away. So that happens all the time.

So what can you do at your company or your clients' companies? First thing is that we recommend -- and the gentleman back here talked

about risk assessment plans or risk assessments, and so one of the first things you can do is identify what information you have. Where is it stored? Who has access to it and why?

So, for example, let's say you have an HR department. You can go department by department, if you can. You can go to HR, you can go to accounting, and you ask questions. What information do we have in our HR department? Think to yourself, what information actually has PII in it or personal health information in it? Where do we store that? What security protections are in place? Is it a hard copy document? Is it locked? Is it in a locked room? If it's online, who has access to it? Do people have access to it that don't need to access to it?

As you go through this kind of department by department, you will realize, we probably have some things that we can improve upon, and then you take it step by step. You prioritize, try to figure out where your biggest holes are, and try to start to fix those holes. Develop a written information and security program or a WISP. So this is something that's actually required for any business that has customers in the state of Massachusetts. It's basically a written information security plan that's going to talk about the administrative, the physical, and the technical safeguards that you have in place. This is not something that you should just copy off the internet somewhere, but you should actually look at what you're currently doing, what you can be doing and make sure that your information security program reflects what it is you actually are doing. An incident response plan.

So one thing that's kind of fun that Bruce and I will oftentimes do is we go in and we do these tabletop exercises or basically a mock breach, and we'll sit in the room of people all from the same company, and we will give a scenario. Let's say it's Friday afternoon. This happens. Do you need to do anything? If so, what do you do? Who do you call? And it's always interesting to see these companies, some of whom have incident response plans in place, employees don't know. I don't know who to call. Maybe I -- do I call Susan? And people around the room will talk to each other now. I think maybe we're supposed to call Bob. If Bob's not around, who should I contact? How do I get ahold of Bob if it's after hours on a Friday?

It's kind of fun to do that in a safe environment where you're not dealing with a breach. Because when an actual breach happens and maybe it's an ongoing breach that needs to be remedied immediately, people have to know who to contact. Who is going to be your General Eisenhower? Who's going to lead the breach response? Have those things figured out ahead of time. Make sure they're documented in a plan. Make sure people within the company know about that plan. Periodically evaluate and adjust your written information security plans and your incident response plans to reflect what you're actually doing.

If that incident response plan identifies who is on your breach re-

sponse team but it was three weeks ago and half of those people have left, that's not going to do you a whole lot of good, right?

Implement employee awareness and training. So this relates not only to just making sure are people are aware of these plans, but, again, are they aware -- just basically your best practices that they should be following. So, for example, you meet with people in your HR group. You realize what information they have. You talked about the steps to implement to protect that information. Make sure the employees are actually aware of what they should be doing.

Regularly test or monitor effectiveness of controls. So, for example, let's say you have that policy, all confidential documents, all documents with personal identification information in them, should it be put in a specific disposal box? Have somebody go around some evening when everybody is gone, check the trash cans. You'd be surprised how many people are not following that policy. If that's the case, then you take steps to reeducate.

I had a very interesting conversation the other day with somebody who works for a health care provider, and she knew that I was in this field and said: This is a very hot area. I actually just had to sit through a half-days' worth of online training about HIPAA compliance and had to take an online test at the end, and we are very focused on this.

She was kind of proud of the fact that they have everything under control. Kind of unrelated, we were talking about texting people, no more than five minutes later, and she says, oh, yeah, I'm constantly texting the doctors that I work for.

It's, like, oh, that's interesting. It's, like, what kinds of things are you texting them? And we find that texting is oftentimes the best way to get a quick response. Doctors, they are not going to listen to the voice mail all the time, but sometimes you need just a quick response, you send them a text.

Well, are you texting them patient information? Are you asking questions about patients?

Well, sometimes I guess we are.

You realize this -- okay, this person just sat through a half days' worth of HIPAA training, and this is going on. So you constantly have to be aware of what's actually happening.

Don't just do the training, just write the policy. Find out what people are doing. If they're not acting as they're supposed to act, then you remedy it.

Proactively manage vendor relationships. This is a huge thing that I'm probably going to get short shrift to. You, your clients, or your companies rely on vendors for all sorts of things. Maybe it's payroll. Maybe they serve a human resource function. Maybe it is IT services.

Whatever the case may be, you are providing them with information. You have a legal obligation to make sure when that infor-

mation leaves your hands it is being protected to the best of that third party's ability. As a result, you should be asking some questions.

You shouldn't just hand over information to them. You should make sure your contracts with them, your agreements with them, have procedures in place. Perhaps you're actually going to have security protocols in there that they're going to enact.

You want to make sure you receive notice if they have an event. If they have a breach, you oftentimes are the one that's going to have to notify your employees who are affected or customers who are affected. Who is going pay for that? Make sure that's addressed in your vendor agreements.

A couple steps you can take to reduce your data risk exposure. So, you know, the presentation before us was all about data management and data mining, and this is very much a hot topic. People like to collect the data, and they like to analyze data, and they like to mine data. For some businesses, that is appropriate. But you have to realize, when you have data, it increases the chance that you're going to have a breach. If you do have a breach, it is going to expand the scope of that breach. It is going to expand a number of individuals that you may have to notify. It is going to increase your costs exponentially.

So, one, collect only what you need and only what you're authorized to collect. Two, going down to the bottom here, dispose of it when you don't need it anymore. It's amazing what we keep around our companies.

Safeguard and encrypt. We talked about the importance of encryption earlier. I forgot to mention, the state and federal breach notification laws oftentimes say, you haven't really had a breach if the information was encrypted. Somebody can't access the information, so it's not a breach. So this just encrypting, not only does it help you avoid those awkward conversations with the enforcement agencies, but you may not have to notify anybody to begin with when you encrypt.

Restrict access. Again, to the minimum level necessary.

It's going to be kind of overkill here, but for the general concept of safeguarding transfer, you can still e-mail people. But if you're e-mailing documents or highly sensitive that has personal identification information in them, encrypt it. It's actually not overly difficult. Talk to your IT staffs. This is something that they can make happen.

Basically, what you want to do is kind of whittle the stack. Make sure you have policies and procedures in place to protect it, and just taking those steps will highly reduce your risk exposure.

So any questions?

FROM THE FLOOR: I have two, and they're hopefully short. The first is, as far as the General Eisenhower, do you recommend that that person be someone internal to the infected client or do you recommend

it's outside counsel?

Then the second one has to do with the tabletop exercise and typically how long. Is that a full day? Is it two days or four hours.

MR. WATERS: I guess I will take a stab at that. So starting with the General Eisenhower, so two answers to that. Internally, you want to have somebody who's the point person, and oftentimes that may be in-house counsel. Maybe it's somebody -- your head of risk management, head of information technology, something along those lines, if you want to have somebody internally who's on the ground, knows people, knows the systems. You also know you want to have an attorney involved, typically outside counsel, but somebody particularly when you're dealing with other vendors. You want to have somebody to help cloak everything from the attorney-client privilege. Regardless of who you use, find somebody who's dealt with this before who basically knows the steps you have to go through and what questions you have to ask.

But what we like to do is, we will basically serve as kind of the quarterback of the situation, and we will coordinate the forensic folks. Sometimes there's public relations folks, and when you send out notification, oftentimes you use companies that do that process for you. So we will do that.

If it's a larger breach deal, go with a call center. All of this is kind of cloaked within the attorney-client privilege, but it is certainly helpful for us, and I'm sure other firms as well, if there is -- are one or two people within the company that are our direct contacts. Again, that's with knowing everybody in the company, know the key people, and know the systems.

To your second point, tabletop. It's something that we -- it's moldable depending on who we're dealing with. What we oftentimes do, I would say it would take maybe three hours is kind of a common thing. What we will oftentimes do is talk with the department heads, IT folks, risk management, in-house counsel, sometimes C-level suite, and we'll talk to them about kind of the importance of these topics and generally what they should do. Then we'll run through a couple of mock scenarios, and that may take a few hours.

There are some companies out there, particularly IT companies, that will actually do something more sophisticated. They will break into your systems for you, and you'll have sort of a live breach going on and see if your IT staff can deal with it. Sometimes there's a legal component to that as well. Those may be one- to two-day exercises, but it totally depends -- they also tend to be more expensive, but that's something that's out there as well.

Any other questions? Sir.

FROM THE FLOOR: What is the likelihood that there will be na-

tional legislation on notification around breaches?

MR. WATERS: I think it's likely. It has dragged on for far longer than I think most people thought it would drag on. It seems like there are a couple of hurdles. One of the hurdles is, a lot of the states want to make sure that whatever is enacted is at least as stringent as what they had enacted, and that's been a problem with some of the previous drafts that have gone around.

There's also some issues about kind of state's rights and, okay, we have this federal standard, are we as a state still allowed -- are we preempted somehow? That has been an issue, but there's definitely been a clambering for it.

If you have an online business and you have to look at 40 different -- 47 different state breach notification laws, it's a hassle, right? So I think at some point in time this is something that's going to happen, but it is certainly taking longer than it should.

MR. RADKE: One thought, in my mind, the notification part, quite frankly, is probably the easiest part of a breach. It's all the other stuff that goes on well before the notification that really is the cost and time-consuming part of the issue. The notification part, quite frankly, is fairly easy.

All right. So, in my mind, yes, it'd be great if we've got federal legislation dealing with notification, but it doesn't solve a lot our biggest problems.

FROM THE FLOOR: How about dealing with regulators or AGs from states at the same time dealing with the FTC? I mean, if you have 47 different states, don't you have -- you could be answering to 48 different regulatory or enforcement agencies. It looked like in some cases, the FTC and some of the other states have gotten involved.

How regularly do you see multiple enforcement agencies getting involved?

MR. RADKE: It is not uncommon. I would say it is rare that all 47 states are going to take an interest in you. At the end of the day, there are probably eight to ten states that I would say are more active than others in this area and you're more likely to get questions from.

Then, I think states tend to take a greater interest if a lot of residents of that state are affected. But it's not unusual for us to respond to requests for information from federal enforcement agencies, as well as multiple state agencies all at the same time.

I see we're out of time. We'll stick around after, so if anybody has any questions, feel free to stop by or give us a call. We are happy to answer your questions.

(Applause.)

PROFESSOR SORKIN: I would like to thank our speakers.

We have cookies and refreshments outside, so please join us for a ten-minute breach -- sorry, break.

(Laughter.)