Data Breaches and Their Impact on Litigation and Policy

An IMS Insights Live Panel Event | November 10, 2021

Julie Amos (01:29):

Welcome, everyone. We're happy you could join us today for our live panel event: Data Breaches and Their Impact on Litigation and Policy. Our moderator today is Adam Bloomberg. Adam is a Client Services Advisor with IMS Consulting & Expert Services. He has nearly 30 years of experience in litigation support and has consulted with hundreds of trial teams and corporate clients to develop communication strategies and presentations that educate, inform, and persuade. He creates materials and exhibits for mock trials, focus groups, arbitrations, hearings, and trials. Adam has led trial technology and logistics in more than 1000 proceedings, including Conduit Company versus US Tobacco, the largest antitrust settlement ever collected. Adam, thank you. And over to you.

Adam Bloomberg (02:15):

Thank you, Julie. Welcome to all of you. I'm excited to be here and to moderate this expert discussion on such a timely topic, Cyber Attacks on Businesses and Firms. We here at IMS Consulting & Expert Services are very excited to offer some amazing speakers today. Just a few housekeeping items: you'll see a Q&A button at the bottom of your screen. Feel free to send us questions; we expect to have some time at the end of the panel discussion. But if you do send them, please indicate if you'd like to direct your questions to a particular panelist, or if any panelists can answer the question. If you have a question that does not get answered during the event, we'll do our best to follow up with you afterwards via email. If you drop off or get disconnected, you can join back using the same link you used originally. So this panel discussion will take about an hour.

Bloomberg (03:10):

First, let me introduce Nevada Attorney General Aaron Ford. General Ford is Nevada's 34th Attorney General and the first African American to take statewide constitutional office. He previously served in Nevada State Senate and had been in private practice for many years. Prior to his legal career, he was a public school math teacher. General Ford earned a PhD in Educational Administration before attending law school.

Next, we'll hear from Dr. Edwin Hernandez, who has served as an IMS expert on complex commercial litigation, patent litigation, and IPR matters. And he runs EGLAVATOR, a technology incubator and accelerator that helps startup raise money and bring new products to market. He has a PhD in Computer Engineering and earned a Master's in Electrical and Computer Engineering.

Bloomberg (04:08):

Our third guest is Jennifer Schaller. She is the Managing Director of the National Law Review. Previously she was in house counsel and director at CNA Surety and a Vice President of ION Services Group in

marketing and business development. She served in leadership for the Chicago City group of LMA and on the Women Rainmakers Committee of the American Bar Association.

And finally, joining us today is Ashley Taylor, who is a partner at Troutman Pepper in the Consumer Financial Services practice with a special focus on cybersecurity issues. As a former Deputy Attorney General, he is active in the National Association of Attorneys General. So now, Nevada Attorney General Ford.

General Ford (04:58):

Well, first off, let me say thank you so much for including me. And this is a very serious topic, and I'm looking forward to having the discussion, but a little levity first. Adam has been bossing me around since the beginning of this entire conversation, and I've been waiting to correct him on a couple of things. The first of which is the pronunciation of my name, is A-ron, not Air-un. I do go by A-A-Ron now, because of Key and Peele every once in a while, I do respond to that. And Adam, unless you want the upcharge it's Nev-ad-a, not Nev-ah-da.

Bloomberg (05:29):

Sorry about that one.

Ford (05:30):

I'm into the state. You can say Nevada if you want to, we're going to charge you, I'm just saying. But no, honestly, thanks so much for including me, Adam, and Ashley and others for being on this panel with me. I am Aaron Ford the Nevada Attorney General and happy to discuss these topics. This past year, we've made some significant progress in passing legislation that's related to consumer protection issues in Nevada. Some of these new laws directly and indirectly relate to data breaches. First, we passed legislation that clarifies that a violation of our Security and Privacy of Personal Information Act, Personal Information Act, which is NRS 603A, by the way, is a violation of the Nevada Deceptive Trade Practices Act. This gives my office greater latitude to pursue bad actors in the event of a data breach in Nevada.

Ford (06:20):

We also made a number of updates to our Nevada Deceptive Trade Practices Act that could indirectly assist my office and enforcing causes of actions against cyber-criminals. For example, we enhanced penalties for conduct that targets minors. If a person in violation of the DTPA, Deceptive Trade Practices Act, directs the conduct at a person who is younger than 17 years of age, the court may now impose a civil penalty of up to $12,500 per violation. This enhanced penalty matches that of conduct against the elderly, and so we're very proud of that. We also added unconscionable trade practices to our DTPA. And in this instance, an unconscionable trade practice is one that takes advantage of a person's lack of knowledge, ability, experience, or capacity that either results in the consumer paying too much for or not receiving access to a good or service.

Ford (07:20):

We also have some laws that are specific on data breaches. And in this regard, the Office of Attorney General is responsible for enforcing certain provisions of the Security and Privacy of Personal

Information Act, and the Nevada Deceptive Trade Practices Act. These laws work together to allow us to pursue actions against those who perpetrate data breaches. Again, I'm starting to have a great conversation today. But I am honored to be here and I send to the mic back to you, Adam.

Bloomberg (07:49):

Thank you to Aaron for that. We appreciate your insights, even though I totally mispronounced your name. Appreciate how you guys are addressing cybersecurity and data breaches. Dr. Hernandez, can you give us an idea of what data breaches issues you're encountering in your work?

Dr. Edwin Hernandez (08:08):

Yeah, certainly. Thank you for letting me into this conversation, I think it's going to be very rewarding to hear Nevada making some good progress in data breaches and cyber-criminals. I think we all have the same issue in small businesses, I deal with startups and ventures. And it happens a lot that a small company, a small venture, will have a partner, even under NDA. And they feel very eager to collect information from that particular partner, and sometimes obtain access to their servers, access to code, access to information, access to key personnel. And then, in many unfortunate cases, they're able to replicate that technology and the venture. And that goes in detriment to a largest amount of investment, and the large opportunity costs that startups have today in America.

Hernandez (09:04):

And we need to foster innovation. We have a very difficult patent arena. Data breaches could, basically, diminish the value of their intellectual property to zero; it could sometimes even bankrupt a smaller startup. And I think having very good, highly skill investigators, as part of the teams that when you detect a data breach, and you suspect that it's from a competitor, you suspect espionage, then that's something that needs to be taken very seriously. And we have seen that, at least in Florida, the state of Florida, we lack of very skillful force that can actually do the prosecution. So they have very rudimentary tools. They're not very educated. And in general, they don't really understand the difference between a trade secret or a patent or even a copyright.

Hernandez (09:54):

So that's a big advantage for perpetrators and people that are in this business trying to obtain information from startups. And again, that's one of the main things, especially right now that we have first to invent. Another thing that a perpetrator could do, and you have to be very aware of that, is that if somebody gains access to your trade secrets and intellectual property, and you have decided to keep that as a trade secret, and then somebody else invents that, then you have to run into a problem that you have to show to a court that their patent may be invalid, or they may have to transfer the patent back to you. But that's a higher risk that inventors and innovators in the startup arena are running into. And I wanted to make sure that data breaches and security is taken care from the state level, from the basics, like the police enforcement side as well.

Hernandez (10:46):

And as well for innovators to make sure that whenever they're disclosing information to a third party or potential partner or vendor, they take precautions to make sure that those things don't get in the wrong hands and end up losing money and time and obviously their intellectual property.

Bloomberg (11:03):

Thank you, Dr. Hernandez. That's some good insight. Now we'll hear from Jennifer Schaller, the Managing Director of the National Law Review.

Jennifer Schaller (11:12):

Hi, Adam, thank you very much. And thank you, Dr. Hernandez, for going over some of the trends and things that you're seeing that impact small businesses. The FBI's most recent Internet Crime report, which dates back to 2020, it revealed that there were close to 800,000 reported cybercrime complaints in 2020, with losses exceeding $4.1 billion and those are the ones that are just reported. This represents close to a 70% increase in total complaints over 2019. COVID, as you can imagine, sparked a massive uptick in internet usage, especially for people quickly being relocated to remote offices and oftentimes on unprotected networks. The result is a 300% increase in cybercrimes in various industries since the beginning of the COVID crisis, according to the FBI.

Schaller (12:17):

Some of the hardest industries are small businesses with 43% of the cyberattacks directed at them, mostly coming in through phishing scams. And as Dr. Hernandez also touched on 60% of these small businesses, small to midsize businesses, fail within six months of a cyberattack. The most frequently targeted industries are financial services, as you can imagine. Oftentimes, either within the organization itself, or from affiliated entities such as vendors, or familiar folks, they might have their guard down a bit. Healthcare, government agencies, energy companies, higher education organizations, we'll talk about that a little bit later on.

Schaller (13:11):

One thing I wanted to mention is when cyberattacks are likely to occur, just simply because at the National Law Review, we've actually had people try to attack our site. We generally have two tech people who monitor the balance load on our servers just because that's probably one of the first indicators that an attack is going to take place. And we've had it happen twice in 12 years, both on holidays, once on the 4th of July and once on Thanksgiving. And this seems to track with some of the more recent trends that folks see with cyberattacks. Many of them, the more recent ones happening specifically for a service provider that provided internet, kind of concierge services for smaller companies who may not have their own in house IT departments. It happened on July 2nd, the Friday before this most recent 4th of July.

Schaller (14:13):

So it's a pretty common thing that's going on, as you all know, and it's just something that businesses need to pivot more directly to address. And, obviously, with the various government agencies here are well aware of, trying to pivot and protect both businesses and consumers. And with that I will send it back.

Bloomberg (14:42):

Thanks, Jennifer. That's some good insight there and how expensive and frequent these attacks are. So now we'll hear from Ashley Taylor at Troutman Pepper.

Ashley Taylor (14:52):

Thank you, Adam. And thank you, IMS for putting this great panel together and allowing me to participate. I thought I would start my comments by trying to provide some context. I left the office of the Attorney General after serving as Deputy AG in Virginia in 2001 to join the firm I'm currently with. And shortly after returning to private practice, I was engaged to defend a company that you all may recall, they have since been purchased, called Choice Point. And I represented Choice Point in the context of what most folks considered to be the first significant data breach resulting in a large investigation. You all may recall, there was a settlement with the FTC and then a settlement with more than 40 states. And I worked on that matter on behalf of Choice Point.

Taylor (15:43):

So I entered this world in the 2003–2004 timeframe, and have been practicing in this space ever since, defending companies. The narrative in 2003–2004 around Choice Point was pretty straightforward, sensitive information that in that case was being sold without sufficient safeguards and protections, security protocols, screening mechanisms, before the information then deemed “sensitive information” was given to a customer. That was the broad narrative. I went back and looked at the agreement and it now looks rather quaint. If you look at that agreement, we had to negotiate the new security protocols reflected in the agreement. And they included physical inspection of an office before someone could be on boarded as a customer, right? The notion of physically going to someone's office in today's world, again, seems rather quaint, but it shows you how much we have evolved and the distance that this issue has traveled.

Taylor (16:48):

But some things have not changed. So there are three specific things I wanted to share that have not changed since that time. First, regulators take, in effect, a strict liability standard. If there was a breach, the information security protocols, by default, were insufficient. That's something that I don't necessarily subscribe to. But philosophically, that's where most investigations start. The second thing that holds true since that Choice Point incident is that companies need to develop risk-based compliance. And what I mean by risk-based compliance protocols is that you have to have compliance programs that reflect the nature of the data that you hold, and the nature of your customer base. And regulators expect you to have protocols commensurate with the information you hold.

Taylor (17:46):

The third item that remains consistent, it really started with Choice Point and it has continued today. When companies want to understand the “law” in this area, it's a combination of statutes and regulations. But perhaps most importantly, it's a combination of the Common Law of Settlements. You need to read the resolutions, and you need to read the injunctive relief. And that really shapes the contours for a company as they developed their compliance protocols. Those are the three things that are the same. There are a couple of things that are now different. One, you see an inherent value argument that is, particularly in the plaintiff’s world, an argument that one's privacy has some inherent value. And what do I mean by that? It's something as simple as if you provide your email address to a company for purposes of receiving 10% off, that there has been an exchange of value.

Taylor (18:47):

So you see now in various class action lawsuits, some of which we're involved in, this argument of inherent value being advanced by plaintiffs lawyers that hasn't been fully embraced by the courts. But you can see that argument being developed. The other thing that has changed is that coming out of Choice Point, there are a series of statutes that were passed, identifying PII, PHI, sensitive information, combination of data points, giving rise to sensitive information. All of that made sense at the time. What's now being argued, is that non-sensitive information, indeed, public information: voting records, your home address, the value of your home, whether or not you have a mortgage. Publicly available information, brought together in the right combination, creates a qualitatively different product worthy of protection. That's the next, I think, engagement in this area.

Taylor (19:48):

And what's interesting is that it surrounds and relates to all publicly available information that folds right into a lot of public record litigation that we're involved in, but I think it's something everyone should watch. People used to feel safe when they are dealing with public records. But that is no longer the case when they're brought together in a certain combination. So those are three things that have remained the same since 2003–2004. And two things that we see are evolving and different.

Bloomberg (20:19):

Thanks, Ashley. Appreciate that. And thanks to everybody for this robust discussion. I'd like to move to some questions here. And Ashley, I'm going to pick on you right away. How are state laws addressing data breaches?

Taylor (20:42):

In addition to the state law that General Ford described, there are three other state laws regulating information privacy practices that I'll focus my comments on: California, Virginia, and Colorado. And in 2018, California passed the first of these laws, the California Consumer Privacy Act, which was amended in 2020 by the California Privacy Rights Act. Virginia passed similar legislation, the Virginia Consumer Data Protection Act, in early 2021, and Colorado followed by passing the Colorado Privacy Act in June. The CCPA is currently in effect, and the other laws will be effective in January of 2023. These laws are all derived from the same set of core principles, the Fair Information Practice Principles. These are essentially guidelines that represent how organizations should collect and use personal information, and include recommended safeguards to ensure data collection is both fair and transparent.

Taylor (21:47):

But there are some differences among the state laws, different terminology, but essentially, they apply to entities that process or control a certain amount of personal information. And personal information in this context generally means any information linked or reasonably linked to an identifiable purpose. Again, a more broad and expansive definition of personal and sensitive information. The laws impose various obligations on these businesses, including notice and disclosure obligations and data processing obligations. Importantly, for our purposes here today, these laws also impose obligations that cover businesses to establish, implement and maintain reasonable administrative technical and physical data security practices to protect the confidential integrity and accessibility of the personal data. In other words, you have an obligation under state law beyond the traditional consumer protection statutes to protect against data breaches.

Taylor (22:47):

Most importantly, the Virginia and the Colorado laws do not create private causes of action. They are only enforceable by the State Attorney General in those states, again, demonstrating how Attorney Generals are at the forefront of the privacy law enforcement. California law, however, creates a limited private right of action in the context of data breaches. The laws also provides significant authority to state AGs to enact regulations to fill gaps in the legislation. Most folks don't appreciate the fact that an AG's office has both enforcement authority and the authority to act as a regulator. So most AG offices have the authority to promulgate regulations and this is one great example. As a result, the State Attorney Generals will have significant input in how these laws are put into action, both through the creation of regulations that businesses will have to follow and through enforcement actions I think you'll see over the coming year. Adam.

Bloomberg (23:44):

Thank you, Ashley. Jennifer, would you like to comment?

Schaller (23:50):

Sure, after I unmute myself. Thank you, Ashley. And thank you, Adam. I just want to briefly discuss the patchwork of state laws because there's been a lot of activity in this in 2021. As of October, nine states amended their state laws regarding the notice requirements, just alone, on how particular companies need to disclose if there's a breach. For example, there... It's kind of all over the block, meaning the definitions of what is personal information, which Ashley touched on. Increasing reporting content requirements, meaning how much you need to report. Regulating the insurance industry, meaning there's a lot of different states that are starting to implement guidelines regarding the type of insurance that can be provided for breaches and laws related to that and it's again all over the block. And as a former insurance person, I don't even know where you'd start with trying to determine the status of the breach. So that's a whole other kettle of fish for insurance nerds to discuss.

Schaller (25:10):

How to handle this different notification timeframes within different states. And one of the things that's most interesting, maybe from a PR standpoint more so, is the Attorney General's requirements to publish on what some folks call a wall of shame, data breaches that have been identified in their state. And then the issue with that is like, for example, Texas recently signed into law that you need to, the Attorney General needs to notify and include on their website breaches related to 250 or more Texas residents, where California has a similar requirement but it impacts breaches of 500 or more California residents. So it's kind of all over the block. And then of the 11 states that I just referenced that have made changes, only two of them have actual requirements to put postings on their Attorney General website regarding breaches. So where I'm going with that is as a business owner, it's kind of all over the block what your requirements are in the event you do have a breach and how to kind of manage that. And with that, I will turn it back to Adam.

Bloomberg (26:32):

Thank you. General Ford, can you discuss what states can do to protect businesses?

Ford (26:38):

Absolutely. Here in Nevada, we believe that the first line of defense against cyberattacks is education. It sounds cliché, but we think that that's absolutely the first line of defense. And that's why we engage in

so much public outreach on these issues. So throughout the last several years, we prioritized providing information to small businesses about cybersecurity through outreach events and online education. In partnership with our Technological Crimes Advisory Board, we created a series of videos as well as a toolkit for small businesses, so that they can arm themselves with the tools to prevent cyberattacks. While the law and my office enforces generally addresses protections for consumers, data collectors who take reasonable security measures are provided safe harbor in the event of unauthorized access to data that's stored on their systems.

Ford (27:31):

Protecting businesses extends to future business owners as well. Before the pandemic, my office also reached out to several local high schools and gave presentations with a goal of persuading our youth to proactively think about privacy risks and the value of personal information, and that includes gaming. Gaming, not in the casino sense, but the online sense, where we know there are a lot of individuals out there who prey in so many different ways on our youth in our communities. And so we've endeavored to educate students, but also the parents on ways to prevent these forms of interactions.

Bloomberg (28:10):

Well, I know that one well, because my 14 year old games all the time, and she says, "Hey, can I log right onto this using my normal email credentials?" It's crazy. Thank you, Dr. Ford or General Ford. Dr. Hernandez, would you like to comment here? And you're on mute.

Hernandez (28:36):

Thank you letting me know that. Thank you.

Ford (28:36):

I'm the only one so far who hasn't messed up and we will keep it that way. And you can call me Dr., Adam, I respond to that. Especially, since you can't pronounce Aaron. But that's just fine. I'm sorry.

Bloomberg (28:46):

Wow. Okay, I'm going to mute myself now.

Hernandez (28:49):

Thank you General Ford. So yeah. So touching on what was said before, as part of the small business, I think it's crucial to have policies in place besides education. I think we notice a lot of attacks every day, they come in from multiple sources, they're getting more sophisticated and more complex. So one of the recommendations I will provide to small business owners is that you pay for a little bit of money, like have a little more budget, to have any of the tools or artificial intelligence, or there are multiple startups that are very well funded, that had developed different management endpoints, basically, to track attacks into your software. Maybe you do some audits, maybe you conduct some sort of technical analysis to your systems, so you can at least have an idea where the attackers could be coming from and what the attackers are looking after in your business. So that's crucial to know and understand at least maybe, besides the education side, it's an investment from consumers. Those tools are actually very, very expensive at the moment. I just went to a cybersecurity conference yesterday, by the way, and the cost is extensive.

Hernandez (30:01):

But I think it's an opportunity both for those small business and startups to innovate in that field. Because as we can say, there are differences in the law that could be automated in software, right. And at the same time, create new ideas and new ventures that could automate the... Understand what happened in every state, try to submit those data breaches as soon as possible. Because you have 30 days in Florida, I think it's $1000 after, a fine. If you go to 180 days it's like half a million dollars, it's a significant amount. So it's worth it for business owners to review the law, understand it, and take some precautions. Back to you, Adam.

Bloomberg (30:40):

All right, thanks. Okay. All good responses here. Let's move on to the next one. Jennifer, this one's going to be for you. Can you tell us about current events and news on any big recent cyberattacks?

Schaller (30:55):

Well, there's so little to cover there. Just some of the more fun and noteworthy ones and ones that might resonate with the most folks in the audience. One that's pretty common or that's been occurring quite a bit is related to the Microsoft email exchange in small businesses. There's a series of breaches from a group called Ragnar Locker Ransomware game and they started not only with small businesses, but they've, in 2020, hit upon Portuguese energy company Energias de Portugal (I apologize if I mispronounced that), French maritime transport and logistics companies CMA and CGM, a Japanese game maker named Capcom, computer manufacturer ADATA, aviation manufacturer (which is kind of scary) Dassault Falcon. And one of the more interesting ones is Campari Beverage Group, which you may be familiar with. And Ragnar Locker demanded a $15 million ransom from Campari, which they didn't agree to pay. And it started getting a bit contentious.

Schaller (32:12):

And one of the more fun facts to tie in some other more contemporary news items is that Ragnar Locker used a Facebook ad campaign that they hacked into an ad agency account to kind of shame Campari group into paying the ransom before Facebook caught that, that had been sort of happening. And there's a couple other ones that are going on that are a little more maybe relevant to smaller businesses, in addition to the ones that are going on with Microsoft email. Exchange ransom group known as REvil, which is short for ransomware evil, they targeted an IT management company and I kind of refer to this in my earlier remarks. A Florida based software group called and I apologize if I mispronounce this, Kaseya, which was a managed service provider, which provided services to smaller companies who may not have their own IT department.

Schaller (33:15):

And what they did is they were able to subvert a lot of the safety features that Kaseya had put in place, requested a ransom of $70 million in exchange for a decryption key. After that didn't happen right away, they weren't paying right away, they lowered the ransom to 50 million. And then in July, their entire operation went dark on July 13th. This is the attack that I referred to that happened on July 2nd right before the July 4th weekend. They ended up getting the decryption key from another third party roughly 20 days after the initial attack and were able to unlock nearly 1,500 customers' accounts which were compromised, but that also meant those customers' accounts were locked up from roughly July 2nd until around the third week of July.

Schaller (34:15):

You may have noticed on the news, there's been talk about supply chain disruptions just in the last, since 2017 or the last four years, the four largest global maritime shipping companies have all been hit with cyberattacks. In addition, we have most recently heard about Colonial Pipeline, which is the supplier of 45% of the country's fuel on the East Coast. They did end up paying the Russian group DarkSide $4.3 million in May to get operations back online for their pipeline. The interesting thing is that the DOJ was able to get most of the money back, about $2.3 million of it, which was paid in Bitcoin. And other than just fuel things like... We've heard on the news, the increasing cost of meat and other consumer products. On May 31st, again, also near holiday, the world's largest beef producer, JBS, paid REvil $11 million in Bitcoin to shield the company meat plants from further disruption and to limit potential impact on restaurants and grocery stores. And to prevent the data stolen from them being leaked.

Schaller (35:48):

REvil initially demanded $22 million. So it seems like if you wait it out a bit, you can get the ransom down, if that's something that's tenable for you to do. So, I will turn that back to you, Adam. That's just some of the more fun and interesting highlights though. There's literally thousands of examples that we could go into.

Bloomberg (36:09):

It's a tad scary, I will say. Thanks, Jennifer. Okay, General/Dr. Ford. We got another one for you, are cyberattacks actionable?

Ford (36:20):

Yeah. Like you said, Adam, these are some scary instances going on. And, Jennifer, as I heard you recount some of the most recent examples, I'm just reminded of things that are happening here in Nevada, especially during COVID. I was asked yesterday if COVID presented new challenges for us. And one of the things I indicated was that it exacerbated some old challenges, which is trying to address some of these exact attacks, especially in the context of unemployment insurance. And so, we look for ways in which to protect consumers. And here at the office, we can commence civil actions against both the cyber attackers and the businesses that were negligent in protecting consumers' data. It's important to note that if the Attorney General determines that a data collector took reasonable security measures to protect consumers data, however, our office will not pursue a civil action against them.

Ford (37:13):

For those data collectors who are negligent, however, rest assured that our office will take action through our Deceptive Trade Practices Act, again, which is located in NRS 598, To the extent you want to look that up. Furthermore, it's important to note that data collectors can pursue private rights of action for damages against persons who have unlawfully benefited from personal information that's been obtained by the data collector through the Security and Privacy of Personal Information Act. The NRS referenced there is in 603A. And in those circumstances the court may also order restitution and penalties against the individual that perpetrated the data breach. The difficulty, obviously, in these cases is finding the perpetrator, being able to know who to sue and who to prosecute. And oftentimes, that's not as easy as it should be or it can present, obviously, circumstances in which we are unable to protect consumers in the aftermath of something like this. But the short answer is yes, Adam, there are civil and criminal actions that can be taken here.

Bloomberg (38:18):

Thanks. Ashley, this one appears to be right in your wheelhouse too.

Taylor (38:24):

Well, as General Ford explained, cyberattacks are often considered to be actionable by State Attorneys General. And oftentimes there is a companion civil litigation or multiple civil litigations filed by the individuals who feel they've been harmed in some way. The key point relates to what General Ford said that is, it's not called a safe harbor but it in fact operates like a safe harbor. The regulator wants to know whether or not the company had reasonable security measures in place. And the challenge for a company is to balance that explanation to regulate at the same time that you are likely defending yourself in federal court, in the public domain. So that's the challenge most companies are facing in the context of having a serious incident. It's interesting to note that in many cases, the companies themselves have been subject to the attack. And yet they're often required to defend not just against lawsuits, but also the government actions.

Taylor (39:30):

And so the government, by way of regulatory action defends our citizens. But there seems to be, at least from many companies' perspectives, somewhat of an imbalance. That is ransomware and cyberattacks are increasingly prevalent. And those companies seem to be victimized twice, at least from their perspective. In fact, I've had one client say to me recently, that if a foreign government physically attacked my company headquarters, all of the regulators would come to my defense, both state, local, and federal. But that if a sophisticated criminal enterprise backed by foreign government attacks, my privacy policies, even if I demonstrate that it was supported by a foreign government, the relationship I have with my regulators is not one of defending the actual shoulder but having to explain whether or not my security protocols were reasonable. That's a tension that most governments or most companies, rather, face. And I know that most companies hope there'll be a broader conversation about how we perhaps should rethink that in the context of cybersecurity.

Bloomberg (40:48):

Thank you, and thanks for the information, something that all of us should know if we're targeted now. General Ford, I know you have to get going here. But we've got one last question for you, if you don't mind. What duties and liabilities do companies have to clients and customers and patients whose information was disclosed?

Ford (41:13):

I appreciate the question and again, appreciate the opportunity to be with everyone. I hate to have to leave early. But it's been fascinating and thank you so much. But to answer your question, a data collector in Nevada, under Nevada law that maintains records of personal information of any Nevadan, must follow reasonable security measures. You've heard Ashley mentioned this phrase. I think you've heard Dr. Hernandez as well as Jennifer mention that phrase, reasonable security measures to protect that data. In the event of a data breach, the data collector must notify Nevadans whose encrypted personal information it believes was acquired by an unauthorized person. And data collectors must also do this expediently and without unreasonable delay; therein lies a few of the keys there. If my office determines however, that a data collector has failed to take reasonable precautions, as I've indicated earlier, to keep consumer data safe, we're going to pursue injunctive relief, we're going to pursue civil penalties up to $5,000 per violation, among other remedies that we have.

Ford (42:15):

And this is why it's important for businesses to review the relevant law in Nevada, the Security and Privacy of Personal Information Act, and the resources my office provides to the public to make sure that they are doing their part to reasonably protect consumers data. Although cyberattacks are increasingly common, their frequency provides businesses a benchmark to gauge their own security practices. And so what is reasonable, and I put that in quotes, is always evolving. And businesses should regularly monitor the current standards for network security. Now, as I log off, I want to offer my office as a resource, you can always reach us at (775) 684-1100. That's (775) 684-1100. My Bureau of Consumer Protection is the frontline for all of these types of issues. And we look forward to working with anyone on issues related to this particular topic. So thanks again for having me. I hate to have to run but I really appreciate the conversation. And I wish you all a good afternoon. Thanks everybody.

Bloomberg (43:14):

Appreciate it, General Ford. Thank you.

Amos (43:15):

Thank you.

Bloomberg (43:17):

Okay, so Ashley, I'm sorry to bring it back to you. But what are your thoughts on that?

Taylor (43:22):

Well, there are various state and federal data breach notification laws that impose certain legal obligations to provide notice to individuals whose information was disclosed. However, it's important to realize that there is a tension here as well for those companies between getting notice out as quickly as possible and making sure that the notice is accurate and complete. In some cases, it may simply not be possible to provide notice, say within 72 hours, because the company has yet to determine which individuals' data was impacted, ex-filtrated, or determine what sensitive information was actually involved. And the investigation remains open. Often law enforcement is involved, in which case notice may be further delayed. But state laws often require notice "without unreasonable delay" but it's not always clear where to draw the line. And for anyone who's been involved in responding to an incident, you know that when you are under intense scrutiny and you realize that your data has been exposed, there's a tremendous amount of pressure to get the notice out as quickly as possible.

Taylor (44:30):

But the worst thing you can do is get an inaccurate notice out the door. You will ultimately be judged, certainly by regulators and by courts in litigation with whether or not... I want to go back to a term that General Ford just used, benchmarking, for example, relative to similar incidents, were you acting reasonably were you acting responsibly? So for concrete touchstones, your incident protocols, did you have them written down and did you follow them? Did you have pre-planning in place, for example, tabletop exercises every quarter? Did you hire competent third party experts? Did you have competent breach coach advice from a legal perspective? Those factors will be the factors that will be used to determine whether or not your response time is "reasonable" in the circumstances.

Bloomberg (45:23):

Thanks, Ashley, I appreciate that. Okay, so I'm going to Dr. Hernandez, any potential best practices for small businesses you recommend?

Hernandez (45:34):

Yes, I recommend different best practices. Number one is to determine... The number one problem I've seen in this small business is a phishing attack. So phishing attacks are probably the most predominant attacks to obtain information from inside your business, try to see what the birthdays or the name of your pet, the name of... What is called social engineering. So phishing attacks, to me, that will be the first line of defense, there are multiple open source tools. And even we have a startup here locally in the building that offers a device that prevents phishing attacks. So even if you receive an email in certainly your company or within your office space, and you try to click on that, it will know it's a phishing attack. So then it will prevent the user from heading over to that website and impersonating your Google account, impersonating your Gmail account, for example, or your access to your bank, that will be very, very bad.

Hernandez (46:32):

So that will be the first line of defense, the second line of defense will be to obtain access to a security monitoring service. So there are multiple sites online that you can pay a subscription base where they will do like... They call it White Hat Attack. So the hackers will pretend to be the bad guys and will try to see if you have basic security measures in that particular website, your domain, or your organization. So those will be the two main things that I will say for a small business, they can be affordable, and something that you will have to do right away. Don't hesitate spending the money on that. And, of course, if you're in a large organization, then you can hire a more sophisticated company to perform those functions. And maybe you need to hire and nominate a Chief Security Officer for your organization that is constantly reviewing the security policies, data breaches, and all potential cybercrime that could occur within your realm. Back to you, Adam.

Bloomberg (47:31):

Okay, thank you. Ashley, I'm going to pick on you again. Ultimately, who will be the primary regulator of privacy? I mean, will we have a patchwork of state laws, a federal floor plus variety of additional state requirements or uniform policy following kind of the model set in the EU?

Taylor (47:57):

Well, Adam, I think that is playing out in front of us in real time. I think we should all watch the Federal Trade Commission. And we should all watch the collective action of State Attorneys General. There is, from my perspective, a healthy regulatory rivalry taking place to determine who will serve as the primary regulator of privacy. The states, as we've discussed, have been passing a number of laws, they did so with respect to the data breach notification law several years ago, now they're passing data privacy laws, specifically. Some, again, creating protocols of action, others limiting the action to the Attorney General's office. At the FTC, there's a debate, actually, in Congress as the role of the FTC. There have been proposals to give the FTC $100 million for purposes of enforcing privacy, specifically.

Taylor (48:57):

There have been proposals to create a new privacy bureau with up to 500 new federal employees with the European model. The question at the federal level is whether it will preempt state laws, and whether or not the FTC and the AGs will have joint authority in this area. Ultimately, I predict that state

law will not be preempted. At some point, perhaps not in the immediate future, but I think at some point we will get a federal privacy law that will provide a floor, but I think we are in an age where the states will jealously guard their ability to put regulations on top of that federal floor. And that companies will have to develop both a compliance protocol and defend actions at both the federal and state level for the foreseeable future.

Bloomberg (49:55):

Great, thank you. Okay, so now we've got a little time for Q&A from our participants. And I'll take the first one here. I think Julie's looking at a few others. But I'll take the first one here. And I think, Dr. Hernandez, this'll probably be for you. We've had the following questions... So here's the following question sent from Samuel Fifer. We read about cyber terrorists holding companies ransom for Bitcoin. Have any of you had any success tracing the bad actors? Also, the FBI consistently recommends not paying the ransom, but we also read that some companies would rather pay than being out of business for a few weeks, there have been pressures exerted by shareholder suits?

Hernandez (50:45):

Yeah, sure. Thank you, Adam. Yeah, so I would recommend not paying the ransom. I will say chances are, there is a 95% chance that it is not true. I had that occur in our organization. We had people that have claimed to have control of certain servers, or have access and they will send the passwords as they say, but they happen to be passwords that were a little old. So that means that they got ahold of an old server, or someone hacked into an organization, and they just found an email about your organization there. And they simply believe that you never change your password. So as a side note, always change your password every month. Doesn't matter if you make a slight change, that will be a key recommendation as well. But I don't recommend paying that. And there's something that is almost impossible, to track most of these attacks, because most of these attacks come from other servers that have already been hacked as well.

Hernandez (51:40):

So they may have one server to hack another server to hack them on their server. And then from that server, the last one, they send you an email, and it's better to respond very quickly. But if you think that it's true, then obviously it is true as well that somebody is going to complain about the server that was hacked last, where they send you the email. So then it will be a matter of time that the server will be taken down. And then the ripple effect will fire back to the hacker. So you have to gamble that a little bit. And my recommendation is that you have like maybe little backups for your system, have a load of other servers that are having backups continuously, that you know are functional systems.

Hernandez (52:19):

And before you put the system back online, before you put it back online, run those scans, bring an expert, and make sure that whatever you had in backup can be cleaned. And then you put it back on online, fix all the patches, fix all the bugs. And that will be sufficient for you to maintain your organization in place and avoid paying a ransom to a hacker that is asking for a Bitcoin because obviously, it will be untraceable once you've made the payment. Back to you, Adam.

Bloomberg (52:47):

Thanks. I think, Julie, were there a couple more questions that came in? I'm not seeing them.

Amos (52:52):

Yep.

Bloomberg (52:53):

Okay, go ahead.

Amos (52:55):

There are. And actually I think, Jennifer, did you have anything else to follow up in response to that first question?

Schaller (53:02):

Well, first of all, I'm in no way recommending that anybody pay ransom. But to go into a little more detail about the Colonial Pipeline incident in which Colonial Pipeline opted to pay the ransom, and did manage to get some of the money back. I think it's mostly from reading the news analysis on it. They got lucky. I mean, they got very, very lucky and it wouldn't be a strategy to rely on. Apparently, they were able to track back some of the Bitcoin public ledgers in order to do that. But that seems that the thieves were not very sophisticated, or maybe it's the first time it was tried. And now they've evolved their processes to be a little better. So that won't happen in the future. So it is what it is. But it has happened that they were able to get some of the money back, but I think it was a lucky break.

Amos (54:06):

Thank you. We do have a couple of questions still to go and we have a couple of minutes. So let's see if we can get some responses. Ashley, going to pick on you now. Taking over from Adam. A question. Am I restricted from paying a ransom and who am I required to report it to?

Taylor (54:26):

So you aren't “restricted” as a matter of law at this point. But for the companies that we represent who find themselves to be the target and having to decide whether to pay ransom, it is a very difficult situation. You are between a rock and a hard place. We always recommend involving law enforcement. And then again, we always recommend that you hopefully have had in place an incident protocol that has been modified and developed using the benchmarks that General Ford described. And it's current relative to the most recent thinking on ransom. But it will depend upon whether or not the information that you have as a company is information that you deem vital, or the law enforcement community deems vital to the public interest.

Taylor (55:26):

Those are the types of questions that you will need to ask again, along with your counsel. Because whatever you do, whether you pay the ransom, or don't pay the ransom, you're going to be second guessed, that's the one thing I can promise any company. But frankly, you just have to recognize that and make the best decision you can. But it really emphasizes the need for you to have policies that are current, so that you can fall back on your policies and make good decisions.

Amos (55:54):

Thank you. And one more. This appears to be going for what the goal is. What are hackers looking for? Is it usually money, private, or insider information to disrupt business or government services? Ashley, if you don't mind, taking that one, too, that would be great.

Taylor (56:10):

Sure, historically, and this, again, goes back to the 2003–2004 timeframe. But most hackers were looking for information that they could place on to the dark web and commoditize in the context of identity theft, that was the very traditional model that was used. The more current model is one of encrypting a company's data so that the company must pay to have that information unlocked. Or the reverse is now true, the double ransom and that is, well, if you don't pay to have it unlocked, maybe you will pay me not to disclose it to the public. And I will have the ability to embarrass your company or your company's executives. So you'll pay me either to unlock the data, or you'll pay me not to expose the data. Hackers are very, very creative in that regard.

Amos (57:07):

Thank you again, Ashley. We have answered all of the questions that have come in from the audience. So thank you, panelists. All right. If there are no other questions, we appreciate you are attending our presentation today. Many thanks to our panelists for this very interesting conversation and your quick responses to those incoming questions. We will send everybody an email with the recording of today's discussion. If we didn't get to a question you wanted to ask, the contact information is on the screen and we will endeavor to get back to you if you have any follow up questions via email. Many thanks again to everybody, to moderator, and to our wonderful panelists and to our attendees. I hope everyone has a wonderful rest of your day. Thank you.

Schaller (57:56):

Thank you.

Hernandez (57:56):

Thank you.

Taylor (57:56):

Thank you.