LAW AND BUSINESS TECHNOLOGY: CYBER SECURITY & DATA PRIVACY UPDATE

Panel: Jason Asbury, Maria McClelland, Kris Torgerson, India Vincent, & Jennifer Boling

Moderated by Amanda Sweenty

Amanda Sweenty: We are so glad you could join us. This first panel, as you know, is for Cyber Security in a Data Privacy Breakout, to give you some information about some of the developments in the last twelve to eighteen months in both of these fields. The way that we are going to kick us off is, I'm going to give a brief bullet introduction of our panelists so that you can match faces with the biographies that are in your background materials. Then, we are going to go ahead and kick off a short presentation with a couple of questions. Then, we will open it up to audience participation and questions for the panelists. Then, we will take a short break and break into small groups so you will have private group-on-one time with our panelists to go in depth in some of their subject area expertise.

I'll have you guys wave as I introduce you. Our first panelist is Jason Asbury, and a big congratulations to him because he was named president of Threat Advice in August, so congratulations that is a huge accomplishment. Prior to that, he was a member of Warren Averate Technology Group, which is a large CPA affiliated company. He brings to our discussion, more than eighteen years of experience in the IT industry, as well as consulting and advisory experience with many different industries, including healthcare, IT, finance, legal insurance, and computer science.

Our next panelist is Maria McClelland. Maria has been at Oakridge National Laboratory since 2014. Currently, she is the leader of the Cyber Security Operations and Engineering Group. Prior to joining Oak Ridge, she worked for the Department of Defense for almost twenty years in IT and in Cyber Security. So she's got a wealth of experience for us today. She also holds a master's degree in Information Technology Management and several industry certifications.

Also, from Oak Ridge National Laboratory, Kris Torgerson. Thank you for joining us. Kris is the Chief Information Officer at Oak Ridge [National Laboratory], a promotion he also received last month, so congratulations. We have a very distinguished panel up here, as you can see. Prior to joining Oak Ridge, Kris worked in the private sector for twenty-five years with a very impressive range of experience that expands several different industries including: retail, manufacturing, banking, healthcare and multi-national distribution systems. Kris holds a degree in Computer Information Systems, as well as an MBA from Idaho State. Welcome.

India Vincent. India is a partner and a Chief Privacy Officer for Burr Forman, one of our sponsors today, where she chairs the firm's Intellectual Property and Cybersecurity Practice Group and actively participates in the firm's Corporate Transactions Group and the Blockchain, Cryptocurrency and Electronic Transaction Focus Team. She also brings a wealth of experience to our panel. Prior to law school, she worked as an engineer for Michelin. She earned her law school degree from Cumberland School of Law at Sanford, a Master of Integrated Manufacturing Systems Engineering from North Carolina State and a bachelor's in Electrical Computer Engineering from Clemson. So she is used to wearing orange [laughter].

Our last panelist, but certainly not least, is Ms. Jennifer Bowling. Jennifer is the Southeast Area Director, Cyber Liability Insurance, and Risk Management with Arthur Gallagher Corporation where she specializes in management and professional liability insurance with a concentration in cyber liability, directors and officers liability, employment practices liability and errors and omissions liability. Prior to joining Gallagher, she worked in the software industry and she earned her BA in Business Administrations from Mercer.

So, that should help you match up the faces you have in front of you with the bio[graphies]s you have in your organization. We will take a short break after we get through the bulk of the questions that I've prepared for them and that they have graciously provided to me, and then we will be able to break into small groups.

For the panel, the first question I have for you, as it relates to cybersecurity is, "what do each of you see is the greatest, unrecognized threat an organization or a business faces today?" What I'd like to do is kick off with our areas of expertise. So Jason, then Kris, then Maria, then India and Jennifer.

Jason Asbury: Good morning everybody. I definitely think the greatest threat is the lack of knowledge for a lot of end users. So it's the educational aspects. I've been in the business for a long time, as we said earlier. I've seen a lot of different scenarios unfold and I can tell you that 100% of the time a breach has occurred, it is because an end user has made a mistake. It's clear to me that the weakest link is definitely the end user and that's why we need to be so diligent in educating the end user.

Kris Torgerson: Since he took my answer, I'll go to the next threat. I think one of the big things to be aware of, or sensitive to, is the "not me" attitude. When we look at corporate leadership, when we look at the investment decisions that are being made, the idea is that it's going to be the guy down the street. It will never be me. HR always shows up with a better risk. Every time we risk proof something, every time we make a small investment, the next person who is hired, the next contractor that is employed, the next person that is brought in the house is going to click on something they shouldn't click on. The idea that it's not going to be me is making people poorly invest because the investment of two years ago is not enough because the threat actors are maturing far faster than we are from a competent standpoint.

Maria McClelland: So now that they've both stolen my answers, (laughter) the one thing that I would add to that is technology of convenience. That to me is one of those areas that we don't really recognize. Everyone likes convenience, you have eighty-nine apps on your phone because they are easy. I was talking with Kris this morning about this. I was curious so I looked it up. The average iPhone user opens and utilizes nine apps per day and approximately thirty [apps] per month. That's nine areas for the attackers to get to you every day, thirty per month. So convenience is great for our daily lives, but it increases the platform for the attack. Those are the things that I—I really try to disable any kind of permissions. I have a smartphone, but it's really dumb because I'm paranoid. Another area is the simplicity of weaponization of code. Like ransomware is a service now, malware is a service. You don't even have to be a programmer to really utilize the weapons at your disposal. They really are weapons of mass destruction. You can take down major organizations with a couple of clicks. Those are the things that I see as not necessarily easily recognizable.

India Vincent: I think my answer is consistent with the others but maybe from a slightly different perspective and I would say it's time and money. We all know the users are causing a lot of the breaches we are seeing or are at least at fault in some way. We know where the technology challenges are coming from, but the organizations have got to decide where to put the time and money behind it to be able to take the steps they want to. A few years ago, it was good enough to be able to say, we made some effort, we looked at it, but with all the new regulations from the state level, all being different, that's not always good enough anymore. People don't like to put those resources behind it. It takes a good gut check to invest in that direction.

Jennifer Vincent: I would agree with everything they said. Everybody stole my answers. I would definitely reiterate from an insurance perspective, when I'm talking to clients, you can just see that once you get past the premium and the retentions, they just sort of glaze over and if you start trying to dig in deep—what if this happened to you, or how resilient are you, how many hours are you going to be down—those kinds of questions, you can just see they say our IT folks have that. We just don't have the communication in organizations, some do better than others, but the legal folks, the risk management, or treasury folks, whoever is making those insurance decisions, as well as the IT folks, sometimes you can't get them all in a room together. Everybody wants to hold on to their information, so it's hard to get the organization to be on the same page at times, which leads to the denial, "it's not going to happen to me, we are good." And that's what really scares me.

Amanda Swenty: Following on that question, I have one that you guys didn't expect. I apologize, but playing off of what you guys have just said, it occurred to me. Do you also find that there is a critical lack of a middle layer who can translate between the IT folks and the folks who are either making policy or fiscal decisions or setting those policy determinations going forward? I think we will start with Kris and work our way over. Do you find that to be the case?

Kris Torgerson: One of the things that I often talk about is the idea that accounting has been around since Ebenezer Scrooge and Bob Cratchet. You've got all of these things and it's a very well defined practice. I went to college with a typewriter. My first cell phone was after I was married. Technology is a relatively young field and what you end up having is people who speak tech and don't speak business. I can tell you, if I walk into a room and I don't stop before I sit down with leadership and tell myself, no acronyms, no tech speak, no nothing, I will lose them in the first ninety seconds and I can never regain them. So the idea is that the translation lends. It's more than just a lack of translation, it's actually a barrier where if your tech leadership doesn't have the ability to speak business, you will never get the funding you need. But they will definitely come and lay blame where it rightfully should be laid. The business has to get a little more savvy, but more importantly, the tech folks look for people who can speak business.

India Vincent: Definitely, the tech folks are looking to speak business and trying to make that transition. The example that always jumps into my mind when people raise this, is when we have one person in our firm who is in management and the minute the conversation turns to cybersecurity data breaches, he says, "Just unplug the internet, that will solve the problem." And only half joking. He would drop it if he could. At the same time I think, as management, those people have an obligation to start doing something to educate themselves as well. It's got to be people approaching it from both directions. From the lawyers perspective, working with my clients on this, that's a lot of what they will call me and ask for help with, is trying to bridge that gap. People are definitely looking for help in that area, in trying to find people who can communicate with both sides.

Jennifer Vincent: I definitely think the person, or whatever title, that is in the middle is where organizations are going to ultimately end up going to, especially larger ones. Larger, middle market accounts, they have the resources for that type of person. You need that type of person to be able to communicate from the IT perspective that has the technology side to them but be able to translate that into dollars so that the management side can also understand that if we spend this money, yes it's going to cost X amount of dollars, but by doing so we can generate or save this much money over here, however they need to do it, but you have to be able to figure out a way to translate those two pieces to merge them together to get everybody on the same page.

Jason Asbury: I think from a translations standpoint, there is really a governance problem in industries management hierarchy. That governance problem is that traditionally an organization with a CIO, that CIO has direct oversight of that information security officer and that is not what is supposed to happen.

Amanda Swenty: Can you describe a little bit why?

Jason Asbury: I will, yes. Managing cybersecurity is a risk management role, it's not an IT role. The two are very closely intertwined but there has to be a separation and a lot of small organizations or even larger organizations who, where top leadership, fail to recognize the real threat they are reticent to separate those roles. I can tell you some large institutions, Blue Cross Blue Shield of Alabama, the CSO is a great guy and he is a peer to the CIO at Blue Cross. That is a large organization and they've recognized, we've got to separate this. That CSO answers to the Risk Management Officer which is part of the internal audit division. Governance, in my opinion, is a reason why the translation is lacking and I think that has to be addressed.

Maria McClelland: Ditto (laughter) again they stole my answers.

Amanda Swenty: I think you guys are seeing a couple of themes evolve across a wide variety of experience bases. Something you can take back to your own organizations, when you have a discussion about whether it's corporate governance or how lawyers integrate into that corporate governance discussion, how they look at insuring against problems, and what to do when problems arise. What I'd like to do, is then turn our discussion toward a privacy focus. And again, short answers from each of our panelists. You've likely read about the federal and state efforts to try to provide greater protections to data and to privacy, similar to the European model, which is all in the papers that we have provided for you. What are some of the challenges for firms, businesses and governments (state, local, and federal), as privacy protection law and practices evolve? And we will start with India, then Jennifer and then follow up with our threat experts.

India Vincent: From that side, the big issue is keeping up with everything. At this point with different laws in each of the fifty states, and then the few subject matters that have their federal regulation scheme, just figuring out what your obligations are is a full time job, because the state laws don't just stick with the state were you are located. You've got to deal with every state in which you may have employees, where you may have customers. You are really responsible for knowing those laws across all fifty states. Depending on the kind of day that you may have, you may have additional federal requirements. All the states now have some form of regulation but they are adding to it. California's [regulation] has gotten the most publicity recently. There are others that are pushing it, one is looking at having a safe harbor, which I think is the best thing we could have at this point because businesses are looking for, how do I know I've done the right thing. I would like to see more states headed in that direction and ideally the federal level doing that at some point but I suspect that is way down the road right now. I think keeping up with it, having somebody designated as responsible for keeping up with it is an important part of managing the issue.

Jennifer Vincent: I totally agree with that. I know when GDPR came out earlier this year and went in force, it was like chaos. Our clients were calling: "Do we have coverage for this under our policy, am I compliant?" I'm like, "I don't know, I can't answer that question." I think for my clients, for all the laws and regulations that are changing and being enacted, it's just the cost of compliance. They are going to have to get attorneys involved, and third parties, to make sure that they've got all their systems where they are supposed to be, that they are abiding by all the latest laws and what not, and that they know what to do if there is a breach in different states. I think for my clients, I think the number one is just going to be the expense of making sure that they are compliant.

Jason Asbury: I think, obviously, that everything you guys are saying is right. The landscape is so vast for a lot of organizations that they don't know where to start and where to stop. The best example that I can give you is a manufacturer. One of my favorite clients is a large manufacturer with 30 something different locations, they do international trade and sales. They are a significant operation in the middle of Mississippi and they've got a general counsel that has been with them since he graduated law school, smart guy, but they don't know where to start. And all they are doing is reaching out to folks like me and folks like you guys asking for advice. But the issue for folks is, what do I acknowledge as something that is really important and pressing and what do I allow to sift through? The answer is it's all important and pressing, but at some point businesses have to make that risk management decision. I'm willing to accept this risk, and this is the reason why. To answer the question, I think that landscape itself is the biggest problem.

Maria McClelland: So, again, he stole my landscape. I had written "know your landscape" and then built tricks off of that. As a research facility, we have personnel from all over the world. We hold data from all over the world, so this is one of Kris' most wonderful challenges right now. I will let him talk to the details of that. As far as we are concerned, we have to know our landscape and that's difficult because it is constantly changing. Every time we get new scientists in, every time we pull new projects in, we are having to do a review and figure out what that means to us. Luckily that is mostly his problem. He just tells us what we need to do and he makes sure it happens, but we also do have to make sure it happens because it does affect all of us. So thank you for stealing landscape, you can have matrix.

Kris Torgerson: In the privacy space, I think one of the big concerns—or one of the big challenges—is IT, organizationally, is often underfunded. Within the IT space infosec at best, often times is an afterthought. So, when we start talking about regulation and we start talking about GDPR, and we start talking about this extra territorial reach where the Europeans are going to find American companies and California is going to find Alabama companies. The IT folks are recognizing, "boy we've got some debt." I don't know where the data is. You have an inventory problem where painting the risk is challenging and if you can't overcome that magnitude, that herculean effort and just get started it's easy to get myopic"well the ERP is safe so we are fine." Again the, "not me, we don't have it." We just did an inventory last year where we have personally identifiable information and if I went to my record, it said I had it in thirty plus systems and I was off by a factor of ten. So the stuff that was getting protected for PII, about 10% of what I needed to protect was being protected about a year ago. That was expensive and it was hard, and everybody bucked and snorted and was angry, they didn't want to do it because, well, it's right there in the list and you have to institutionally recognize that it's a collaborative thing. If legal is not in the room, the IT guys can't make a judgement, they are not smart enough. If risk is not in the room—it is a collaborative mosaic of people who have got to be in the room to determine where to start. If no one knows how to start, pick a place and go.

Amanda Swenty: Excellent answers, thank you all. So, we have reached our point where we are going to bring you guys, the audience, into the discussion. So what I'd like to do, while you sit there and form your incredibly insightful questions for our panel, is just give our panel just sort of an indication of the scope of the audience that we have in front of us. Again it's audience participation time. By a show of hands, who within our audience is a law student or a legal professional? Oh, big group. Okay. Who within our group are technology professionals? Excellent. How about federal, state, or local government representatives? Wonderful. Privacy officers? Hmm. How about data management professionals? None there, okay. How many of you are avoiding being at your desk on a Friday? (laughter). How about Florida fans? Just checking. It occurred to me that you guys don't actually know who I am so I should probably remedy that as well. My name is Amanda Sweenty. I will be joining the faculty here in January to help out with cybersecurity, national security, those types of courses that we are building now as part of additions to the curriculum. I've spent over twenty years in federal service and I'm still in federal service so please don't ask me any questions about what the president is doing because I won't be able to comment on that nor would I comment on that. And I do not have a Twitter account, I will be honest about that. I'm really looking forward to joining the faculty here. If you have ideas for the curriculum, please get in touch with me. I think our contact information is in the information that you already have. If there are any questions on the federal level, I'll also do my best to field those with the rest of our panel. So, now that you've had time to formulate your questions while I've been up here tap dancing, what would you like to ask our panel of experts? Either singularly or as a group?

Audience: *Have you guys had any clients wrestling the* GDPR *that just decided to remove their products or services from you, just until they remedy and have the appropriate risk procedures?*

Jason Asbury: I had a client who made the decision to remove any data or any relevant information. They didn't stop trading but they did make the decision to remove any pertinent data that was in scope, "permanently," not "until."

India Vincent: I've had clients do the same thing with the data, I've also had clients use other vendors, where the vendor would not guarantee the data stayed in the United States.

Audience: *When they remove that data, do they remove just European customers or do they just go ahead and whole-scale everything? US?*

Jason Asbury: Mine just removed what was in scope of European relevance.

India Vincent: I have some of both.

Kris Torgerson: Before I came to Oak Ridge, I was in consulting and I actually had a call last week talking about that with a multinational retailer and they are wrestling with what to do because they've got distribution, wholesale, retail in GDPR countries. So, in some instances you can do that. They retail in airports with GDPR. They struggled with that but they were not able to. You've got to close down operations essentially.

Audience: *One thing, and this goes to your ten percent of PAI(inaudible) is where we know it is. One thing that I've experienced is finding that there is PAI outside of bounds of what we normally have and my company has made significant changes to shut down accessed information much of which is necessary for day to day operations and people are individually granted access, almost on a by document basis and it is creating a tremendous amount of unnecessary transactional churn to get things done. Is anybody working on ways to—what are you—might be doing to figure out how to keep the work going? Give people access to the data they need to get their jobs done while still partaking (inaudible) security?*

Kris Torgerson: One of the reasons why I'm in the role that I'm in now is because borrowing the right solution—Maria cringes every time I say this—but we've got to find a right way to do the wrong thing well. I tell my team all the time there wasn't a great IT organization that said, "Heck, we should open a lab." That's not how that worked. From a cyber standpoint, a security standpoint, and a tech standpoint we exist to serve the business and if the business's cash register is not ringing, nobody is buying dinner at night. So we've got to find a way to enable business and that kneejerk reaction to say, "take the old model and apply it harder"—it's that old adage right, if I just say it louder they will finally get it. We are looking—the old model was a role based access system, a lot of people are talking about data-based access system and computationally it's easier to find at a data level and say, "okay, how are we going to control that?" The paradigm has got to shift and it's not shifting briskly because the old role-based access system and broad access to everything. We just had a small incident where we were worried about where our data was flowing about pension funds. Again, it's a daunting thing but you can't stop the business. To answer your question, part of the reason why I'm here is because I won't do that. Finding a way that enables business is critical.

Jason Asbury: I'll add to that as well. A lot of organizations are trying to safeguard information about consolidating it. If you think about it, everybody in here—I see all sorts of laptops. I don't know how many of you are working from your local desktop or you might be remoted into a system were your data is staying in one place. Larger organizations with larger IT budgets, they are investing in software that allows them to consolidate their data and they do all they can to secure that endpoint. You see that little device right there would be encrypted, it would also be managed with mobile device management software. It would have as much of a safeguard protection as can be applied, but at the same time the data would never actually be on that machine. It's always consolidated.

Kris Torgerson: I want to touch on that too because it's the same thing we did. We assumed that it's going to spill, so if it's something you can pick up and carry out of your office, we encrypt it. Because I assume: (a) it's (the data) going to spill; and (b) you are going to leave that (a laptop) in the trunk of your car and someone is going to pop your trunk and it's going to disappear. From a data loss perspective, when it's encrypted, it's a whole different discussion than when it's not.

Jason Asbury: Encryption is a safeguard in most instances.

Amanda Swenty: Following up on that thread as part of our paper discussion, we touched on changes in certain state legislation in terms of how they deal with crypted data versus how they deal with encrypted data. Can you talk just a little bit about that?

India Vincent: Exactly the point that has been made. Under most state statutes, I may get myself in trouble with that. If the data was encrypted at the time that was lost, as long as you can prove the key was separate and the key was not compromised, you will greatly reduce or either eliminate your reporting requirements, particularly if you are talking about healthcare records. That's significant because access is considered a breach for reporting purposes of healthcare data, so encryption is significantly helpful there. Several of the states that are beginning to increase the strength of their laws are taking that approach as well. The arguments we hear about not liking encryption are usually related to user convenience: frustration with users from speed or difficulties getting stuff off of their laptops. In my view, it's because a lot of times people are using the same device for business and for personal for a lot of organizations. It's something that definitely helps the organization, but could be frustrating for the user depending on how well it's done from a technical standpoint.

Jason Asbury: If you don't mind, I'll add a little bit more to that, too. It's really relative to an encryption conversation. A lot of covered entities are requiring that business associates have encryption at rest. Encryption at rest means that the data is always encrypted no matter where it's at. That could even mean on a server in your office. It could mean cloud service, and so on and so forth. Encryption in transit has been around for years and that's pretty common place, and we've got a good handle on it. But I say that about encryption at rest because the shelf life of a breach has increased dramatically from the time that the breach occurs until it is actually identified and exposed. This time a year ago I would have told you it was about 110 days. Today it's about 209 days. If you think about that, if your organization has been breached, and you just found out, and it probably happened 9 months ago, with that in mind, having those safeguards for encryption at rest becomes really essential. If you are on your network, that's one thing, but if you are on a network and you can't get to the data you are trying to steal, that's another.

Audience: *Going back to the days when Al Gore invented the internet, have we grown too fast in terms of this entire technology to the point where we're spilling water over (inaudible) trying to capture something that might not necessarily be (inaudible) from a security standpoint? I raise this because it seems like we're in this unregulated universe of information and I think that regulation—we should be going back to the same responsibility of the companies. Is it time now that we start really thinking about if we're going to operate in this high tech world where everybody has access to it—there's a lot of responsible and irresponsible people using it—that we start placing some burden on who makes up for it, who make up a company so that we don't have rogue companies that are just creating a host for cyber-terrorism that will float its way into the US and society? I guess my question is, have we grown too fast for responsibility of the user who is "Joe Blow" who doesn't fully understand?*

Jason Asbury: I would say we have grown extremely fast. In 2000 when I started my career out of school, I went to work for the Alabama Department of Transportation. I was a consultant because they had a hiring freeze. My point is my boss, I knew pretty well, he put me on the "A" team, and I was with the network guys. Long story short, I walked in and we had this cubicle area, there was a folding table and all the servers that served the whole transportation department were on that folding table and now they have a data room that's three times the size of this room. That's a lot of growth in a little bit of time. That has happened exponentially world wide. I took part in a cyber-symposium in the spring down in Tampa and the keynote speaker was a professor from MIT and the interesting thing that she had to say is that, basically that academic world is trying to find ways to determine, "hey are we doing this the wrong way and should we be attacking cyber security from a whole different lens?" It's been too long for me to get into a lot of detail on that, but the point of the matter is that the academic community and the computer science base is really beginning to take a look at cyber security from a whole different lens because the fact of the matter is we've recognized that we've grown too fast and this thing is almost unmanageable. That doesn't mean you just stop. You do what you can.

Kris Torgerson: I'm going to argue a little bit on a different side there. Three things: (1) as the cost of breach starts to rise—I was just looking at an article where the average cost of a breach to an organization of medium or large size is north of $5.5 million. That is going to shift behavior. The reality is, even if we look at the stagey antiquated—the first cyber security class I took was in the early 90s and the stagey antiquated models that we were using back then—if we look at them today they are not remarkably disimilar, they might be a little more mature but, if you apply the basics, remember IT is underfunded, cyber is materially underfunded. If you apply the basics and you think about your data no matter where it's at in transit, at rest, or in progress, you compartmentalize it. That's one of the things you will see in your paper when we talk about uneffective responsible approach it implementation. There is nothing we can do to control the whim and fancy of politicians. As the regulation comes, if we have the regulation to drive our compliance program, we are always going to be leaning back and reacting. Getting proactive, even if it's the basics—the gardener model, the mercumber model, there's a hundred of them out there—apply it and apply it well. Do encryption, be responsible. The regulation is not going to be the problem. There is nothing we can do to put that genie back in the bag. If you look at the news, downstairs two floors below me, I have the fastest computer in the world by several magnitudes and right now, we just broke ground on a room because we are building a faster one. There is nothing we can do. The reason why we are doing that is because seven or eight months ago China had the two fastest computers in the world. This is like the old space race We don't get to opt out. As much as we would like to shift culbability and liability, the people in this room own cyber and privacy going forward.

Jennifer Vincent: I will say, since I do have the advantage of talking to Ds and Os at companies when we are talking about cyber and directors' and officers' liability, they definitely recognize that they have a play in this. Their personal assets are at stake, especially for, you know, private company or public company. But I will say that I have noticed a trend in boards specifically electing more technology related people to their board or having some sort of, you know, IT person, whatever, you know, that can provide insight to the rest of the board that doesn't have that knowledge.

India Vincent: I'll add to that. It goes to your point about should we be placing more responsibility or liability with those board members. Several of the boards I participate with have been through the insurance discussion. There is awareness on those board members' parts of potential personal liability, and it's interesting to watch the ones who opt to resign from the board because they don't like this risk and can't get comfortable with it. The ones who focus on the insurance and what do we do to make it better and the ones who say it's not going to happen to us.

Amanda Swenty: India, can you also touch just a little bit on the role of lawyers and those discussions and how lawyers can facilitate those conversations?

India Vincent: Okay, in this case I think it depends on if the lawyer is involved with the board, are they there as the board's lawyer or are they there as a member of the board, because you've got different things you need to be focused on from those perspectives. When I'm advising boards and serving as the board's lawyer, there is a lot of discussion about what could your liability be? What have you done to try to make sure this risk doesn't happen to your organization? What are the organization's risk tolerances? There's got to be an awareness and an act of working through that process to decide. For some nonprofits there may an element of, it's not going to be us or we don't have data that is that important. Usually, I don't agree with that. There is something every organization has that somebody wants, even if they only want it for blackmail purposes. You've got to keep that in mind. Is the board's lawyer trying to get them to recognize the risk and be proactive about how to mitigate it? Serving on the boards, my approach is always to make sure those questions are getting asked and to turn to either the technology advisors or the legal advisors for the board and see what kind of answers we're getting. I'll admit there is one board I resigned from because they took the, "it's not me, it's not ever going to be me and we're investing zero dollars in this to try and fix it." But, generally, as a member of the board, I view my approach is to make sure the issues are raised and see if the board addresses it, to do whatever I can from that perspective, but I also have to keep in mind, as a member of the board, it's my personal liability as well.

Audience: *I had a recent vendor audit and there was a finding that the vendor that we were using was storing our information for 30 day periods in the DMZ, or the demilitarized zone, and that was a concept that was new to me. So, basically the way they explained it was this greatly increased the risk of the breach of the confidential customer information. So, I was just wondering if anybody could explain that concept in a little bit more detail and the risks associated with it.*

Kris Torgerson: One of the things that exists in IT is the idea of compartmentalization. So, if you think of your network as a house, you've got a panic room that is really, really safe and you've got a front porch. Think of the DMZ as the front porch. So, I don't put my valuables on the front porch, I put them in the back corner of the panic room. Having the DMZ, there are some safeguards there, but it is designed to be externally exposed. I would never want to store sensitive data, whether it be regulated or not, in a way that it was actually in the DMZ. I would say that that was a significant finding, but if you think about it just in the terms of that architecture, they're storing your data on their front porch.

Maria McClelland: I just have to ask, are you sure? Now you are giving me a heart attack. DMZ, like Kris says is the front porch but it's not just the front porch it's the front porch that says welcome.

Jason Asbury: Well, there's also often a lot of misuse of the term DMZ. A lot people think of—that's an old term a lot of networkers used back in, you know, the day, whenever that was. A lot of people call DMZs, what are really private sectors of a network, they're just compartmentalized at this point. I would think more in terms of a quarantine space where data sits for a period of time to make sure that nothing is there that shouldn't be there and it can be kind of purged and some level of assurance can be put on it that you are not bringing data that you shouldn't be bringing in. So, if I were you, I would ask a few more questions like, "Is this a real DMZ? Where it's internet facing or is this just a quarantine space on a network that has no access to other components of that network?

Maria McClelland: Like an internal DMZ? But still, you shouldn't have data sitting there for 30 days.

Jennifer Vincent: I'll say too, again from an insurance perspective, you will find that carriers are asking more and more questions about vendors. They want to know who the vendors are because they are trying to aggregate it on their end that if they have 90% of their clients have, you know, Dell, whatever, you know, in the background, and Dell were to go down, how is that going to affect them as a carrier? They're doing very diligent work on the underwriting side to find out who your vendors are, what kind of information you potentially have stored there, so they can kind of aggregate on their side.

Audience: *I'll follow up on the vendor question. So, I work at a company that has tons and tons of vendors, and so we will contract for terms with many of them, controlling data, we operate in all 50 states and Canada. And so, I'm a lawyer, and we look at contracts all the time, but I'm wondering from a risk perspective, how often should we be auditing the security of those vendors—long-standing vendors that we've operated with and have master service agreements with them? Like, how often is this landscape changing where we need to be looking at our insurance—the newest PCI compliant—whatever the issue is?*

Jennifer Vincent: I would say—speaking from an insurance perspective—what the insurance companies usually ask for, but they at least want to see an annual audit of all vendors but you can rotate them so it's a constant sort of rolling of, you know, when you're auditing them, but they definitely want to see, you know, at least an annual audit of vendors.

Jason Asbury: A lot of organizations are able to bypass a number of those audits if a vendor is able to present certain credentials through certification. And those certification credentials require audits on their side, so that expense is on them instead of on you. A SOC1, SOC2, ISO, ECI, all that.

Kris Torgerson: Yeah, I think that is a good point. Even within your Ts and Cs, start thinking about if you require and what type of certifications you require of your partners, because, to his point SSAE16 or SOC 1, SOC2s tell you a lot about the integrity in the design. I would definitely have some requirements and if there are none, or they can't do that, you need to audit.

Amanda Swenty: I have one request from our taping crew, when you ask your questions, please speak up because the CLE is being recorded for later rebroadcast.

Audience: *I'm so angry and I don't know if I can ask the question appropriately. It's sort of a two-part question. The risk management side indicated that some people are making this decision almost as if we've just got to figure out what the risk is and whether we want to put the money up. How in the world can they make this decision, because I'm not sure that even if the insurance company—if the liabilities are changing so fast, the cost of the breaches are so different or often times kept secret—how do you even put a number value on risk? How much is this going cost? How do* *we decide whether it's worth spending the money on security or not? They've got to come up with some numbers somewhere. Where do they get the numbers?*

Jennifer Vincent: Well I'll say, again from an insurance perspective, I mean you use the information you have, right? So where they are making decisions based on information that has been provided to them either from, you know, internally, as far as record counts, or, you know from a network perspective, you know, what their vulnerability, you know, is. And then they use that information, coupled with information that we get from the insurance carriers, from benchmarking with their peers, of just how much they're buying. So, I mean as far as purchasing insurance, those are the factors that they're using and we try to drill down as much as we can, in their particular industry, with their particular size company so they know how much to buy. But, I mean I will say, the big cyber event really hasn't happened yet from an insurance perspective. And I think the carriers are preparing themselves for it, and that's what I worry about because, you know, there are, you know, so many law firms that are sort of the top tier that handle breaches and whatnot. There are certain, you know, vendors that they all have on their panels, and so, if we have the big one, I don't know how that's, how that's going to work. I worry about that. Purchasing decisions on insurance comes from benchmarking and just what they do know.

India Vincent: Along the same lines, I think the insurance question may be coming sooner than we think. We're seeing a lot of cases right now arguing over whether or not something was covered under a particular policy. They're hitting the Court of Appeals level now. We've got the circuit splits already in existence. The social engineering is a big one, and whether it's social engineering or whether it's computer fraud. Forensic analysts are spending a lot of time digging into that trying to prove how they get into one system or the other. To your point, the thing to keep in mind is there is cost for somebody associated with those forensic analysts or with those court cases. Usually, if you think there's a possibility you are going to get into and lawsuit over this, and you can't stop people of suing you, you've got to assume the risk is going to be fairly significant. Depending on the type of data you are housing, you may be able to say we're high, medium, or low, but everybody has some level of risk there to be focused on.

Jennifer Vincent: And the cost for the analyst and the attorneys, all that, obviously, is continuing to rise.

Amanda Swenty: Did you have a second part to your question? As gloomy as that is, as a gag gift when I left my last job advising one of our senior tech professionals—as he would come in and ask questions that

I couldn't possibly answer, not just from a legal perspective but just from a substantive standpoint. So when I left, I got him a Magic 8 Ball to answer his questions. And sadly, when you're weighing a lot of these options you just don't know what the "but if" answer is.

Audience: *So, what you are saying basically, many years ago when I was a young associate the litigation section presented a case who was really bad in the hospital and they said how much do you think the jury might award and the answer was basically how big can your imagination go, that's basically what you're telling us. That the numbers are so broad—I mean some companies are looking at getting wiped out if they don't handle things the right way.*

Jason Asbury: Over 60% of companies that are breached don't survive.

India Vincent: More than a year. Yeah, they are out of business within 12 months.

Jennifer Vincent: Which I think ties us all back to, why at the beginning—what makes us nervous is the people being in denial that it's not going to happen to them.

Audience: *Now that we've all been scared straight. Could you talk about eliminating, litigating, insuring against, and having contractual indemnities as ways of managing different risks, and what trends do you see in vendor indemnities or even in mergers and acquisitions agreements for representations of warranties?*

Maria McClelland: So I'm not a lawyer, and I will tell you my focus has been cybersecurity emerging threats and trying to defend against those on a daily basis. So, I cannot speak to any of the law. I will tell you that Kris and I were talking this morning. I give threat briefs all the time for both of my positions and I like to scare people because they don't pay attention until it happens to them. I'm a prime example. I turn off everything, I use VPN on my own, I encrypt everything, and I don't use anything that I don't have to because I've been on the other side, and I know how easy it is to get into. So, I'm paranoid when it comes to my banking as well, but we were overseas and my husband happened to use his bankcard to buy a soda or something. A month later—and I give these briefings all the time—a month later I started getting text messages from my bank saying that, you know, all of these charges were coming. I saw my checking account and my savings account wiped out within minutes. So, sometimes there's nothing you can do. I contacted the bank and it took weeks to get the money back. They never found out how it happened, and this is what I do on a daily basis. There's really no way to say when it's going to happen, who it's going to happen to, or how it's going to happen. It just does. So, how do you insure against that? I have no idea because you can't tell how much it's going to cost and how much it's going to cost in forensics. We do forensics investigations all the time for our lawyers and they're starting to understand more about what we do, and we have a very good relationship with our general counsel at [Oak Ridge National Lab], and we're starting to get a lot closer to them because as they understand what they need from us, they understand how much bigger it really is. I have no clue how to fix that.

Jason Asbury: I can say, as it relates to vendor management, that a lot of the larger organizations out there are really trying to push that liability and extend it to their vendors, and they are doing that contractually. They are doing it either through those master service agreements, many of them have an ISA (information security agreement), as well as in healthcare, you know, business associate agreements. I've worked with a number of organizations, especially law firms who have done work for, you know, Walmart, Geico, State Farm and so on and so forth. And, you know, the trend is definitely that liability is being shifted to the vendor. I can't speak on the legal aspects, but I can tell you that I'm seeing it.

Jennifer Vincent: I would echo that—Our clients look to us. You know, we'll review contracts from an insurance perspective, and, you know, we're always reminding them to read their contracts because sometimes they just—they need the business, you know, and they're gonna sign off on it. But, wherever they can, push the liability off. But, sometimes if you're, you know, a law firm and you're wanting to work with Bank of America or Walmart or whatever, at some point you are just going to have to say, "Okay, we're doing what we can do, but we're gonna take the risk." And that's just the decision you have to make.

India Vincent: I think that both in the M&A setting and in the vendor contract, that unfortunately you're not coming down purely to who has the leverage at this case in most of the ones I see. The customer, as they've indicated is always pushing the risk to the vendor, right now. I would say 95% of the time I see those contracts come through at the first pass putting 100% of the liability, regardless of fault, on the vendor. Most of the time there's some push back on that, and there's a lot of discussion about, well if we mitigate this to say whoever was at fault for the breach, whoever failed to secure something they should have, they're responsible. The more sophisticated ones go from there to a discussion of how do we figure out who is at fault and how much are we going to invest figuring out who is at fault or are we just going to say we split it. Lots of discussions going on along those lines. But the larger vendors, you mentioned the banks, they're just saying, "No you're responsible" and you either do business with them or you don't.

Jennifer Vincent: I will say from an insurance perspective that representations and warranties sales have picked up. So, and I don't know if that happened after the Yahoo situation or what, but I've personally noticed it in the last eighteen or so months. A lot more questions have come in on the representations and warranties coverage.

India Vincent: And that ties back to the point of how long it's taking to discover breaches and in the M&A situation you are seeing the representation that we're not aware of and there haven't been any breaches in the last three years that are going to cause liability to the company. From the perspective of the party making that representation, there's always that risk. You may be 90% certain there is nothing in your system, but you are never 100% certain.

Kris Torgerson: I think two things that I'd add also. We just got done with two years of figuring out ISAs and systems of record and who retains the business associate agreements on one of our research projects. And this research project, you know, has the course to change the course of humanity from a medical treatment standpoint. Two years getting that liability figured out. You have to recognize that the stakes are incredibly high. Frankly the biggest concern, at least from my perspective both as privacy officer and information officer, isn't really the legal culpability or the liability but it's the reputational risk. My first career was in public relations and I remember the old days back in the 90s when it was there's no such thing as bad publicity, well that's crap. That's a bad answer. You have to recognize that there is a reputational risk on top of having an agreement. The entity we are working with on this, because of those two years, we have a far better relationship, we have a far better trust and frankly the security plan as a result of those discussions and recognizing who is culpable for what—If it ever gets to the contracts, you have already lost. The idea is to use that as a mechanism to build a relationship because this is scary stuff, and you do not want a bad day.

Amanda Swenty: We have 2 more questions on deck. I think you had one and you had one, right? Please go ahead.

Audience: *I'm an associate in-house at a vendor, actually. We offshore insurance services to another country. We have ISO certification for information security. Recently, we had some customers or prospects come forward and say we prefer SOC, we have heard this is higher security. We are under the impression based on what we have that there may be similar in scope, they are are different pools, one may not necessarily be better than the other. SOC is more focused on accounting standands and procedures, and ISO is more information, security, and technology based. Do you have anything to* *say about that view point, the differences between the two? And to what extent are the standards not comprehensive?*

Jason Asbury: I can speak on that. Part of this role, I was with an accounting firm and I ran our SOC practice. That service [SOC] is about process so if you do the same thing day in and day out, that SOC certification basically validates that you do it correctly, that you are following industry standards and you are consistent in doing so. So, when you say it is accounting oriented that is the reason why—it is making sure you are doing the same thing time and again. ISO is quality based. An ISO certification says, not only do you follow these processes, but you also have the highest level of quality that you can have as you apply those processes. It depends on who is interpreting which one has more weight in order of difficulty to achieve. The SOC is difficult but it is not as hard, usually. The SOC is on your way up to the ISO. If you have an ISO certification that is pretty impressive.

Amanda Swenty: Great. Do we have other questions? No. Okay, so that means that we are into the lightening round. I have one last question, as if this wasn't enough to keep you up at night. I would like to go through our panelists starting with Maria and ask each of them individually, what does keep you up at night? What's the thing that scares you the most?

Maria McClelland: So that one is easy for me. It is what I do not know. We spend all of our time studying, looking, and watching, trying to figure out how to make the next move. This is a chess game. It is definitely a chess game. Someone back there said something earlier about the speed in which technology is growing. That is great but it is also really scary because we cannot secure fast enough. Our entire mission at the lab is enabling research. As cyber security, my job is to contain as much as possible while still sharing with the rest of the world. That is what keeps me up at night—What am I not seeing? We see hundreds of thousands of events a day. We are pulling in terabytes of data. We are watching and tracking and monitoring all of the different user behavior and all of the different networks. We are seeing all of this stuff, but what am I not seeing? That is what keeps me up at night. I know it is there, it is just one of those things that you know that they are there but you do not know they are there. It is what I do not see.

Jason Asbury: For me, I will go back to the first thing I said and that is the end user. At the end of the day, the technology itself controls what we can put in place of technology are pretty sophisticated and advanced and the truth of the matter is, they work. If they didn't work, today's trends would not be based on user breach. That is where it really is. When you think about fishing, malware, all of that stuff—How do you get a user to do something that they should not do? So, the technology really does work, it is really a question of how much money do you want to spend. At what point does the technology begin to impede your ability to conduct business? There comes that risk management conversation. But for me it is definitely that end user. It is very clear to me that we have to educate the populous as much as we can. The problem with that is, too, that education can't stop. Just like you guys are here for a CLE today, it has to continue because things change.

Maria McClelland: I would add to that because I had written that earlier. End user definitely, but also we tend to get complacent as we build our systems out. We play with new technology but we forget—a complacent sysadmin can be more dangerous than an end user, because we are configuring these systems and then we just use default password, or we leave something open or we forget to patch it because I am tired, I have worked twelve hours today, that is when that exploit hits. Those, in addition to an end user, are humans.

Jason Asbury: I tell people in the conversation, in the vein of the CSO should not report to the CIO. No one wants to tell someone their baby is ugly. CSOs have the tell the CIOs, "Hey, this thing needs a diaper change," and they do not like hearing that. That really speaks to that complacency.

Jennifer Vincent: Mine might be a little more doom and gloom, I do not know. Probably because I read from so many reports, I get energy, utility reports, banking and financial type reports of things that happen or could happen. My lay awake worry is nation state attacks on your utility system and our banking systems, such as, what if we wake up and everything is shut off? What are we going to do? That is what scares me.

India Vincent: That is gloom and doom. I am going to say this acknowledging that most of the hands went up as legal professionals, but trying to manage these kinds of issues for a large group of lawyers. We like new technical gadgets. Anything that makes it easier for us to be more mobile, to get data to our clients more quickly. I talked with one CIO at a law firm recently and he said that he wished that when his lawyers went home at night, they could not watch TV because he was tired of the latest greatest gadget walking in the next morning saying connect this to our system for me. You read all the predictions that say the next big breach is likely to be within the law firm field. That is what worries me.

Kris Torgerson: When I was a freshly minted IT executive, the first real executive position I had, I started to conference a lot. I ended up at this conference, and I went to this little classroom and they handed out a pamphlet. It was a ten page document on how to hack an active point of sale in retail. And I giggled and chuckled and looked through this thing, and when I got back to the hotel and logged in the used case was my point of sale at my company. We were a $5 billion a year company and a used case at a hacker conference had printed material was my system. When Maria talks about the unknown, we underestimate the adversary. You talked about a nation state attack. The little festivities have been going on in the Baltic for a while and probably the most effective cyber weapon deployed was NotPetya—$10 billion, shut down a country. By the time they saw there was a problem, the data center was gone. Somewhere in some hacker conference, there is a ten page document that tells them how to get in my house. That is what keeps me awake at night because it is not IF it is going to happen. That is the one thing that I would—I just do not know what it is going to be when it happens again.

Amanda Swenty: One follow-up question.

For old people like us… (inaudible). The fact that Y2K fizzled give bolsters what was around at the time. I remember the stories in '98 and '99 the dotcom bubble was bad enough when the Y2K spending went through the roof, and then everything crashed and burned because nobody needed IT for the next three or four years. That is the bottom line for the average person out there, it scared the heck out of us. It turned out to be a big joke. So, we hear these stories but we have heard these stories before. Is that a problem you deal with all the time with your clients?

Kris Torgerson: It is interesting because I made a lot of money in '98 and '99, slinging a lot of code.. There are two schools of thought. The one school of thought is that it was a fizzle, and it was a nonevent. I saw it a lot in the early 2000s that you are in here crying wolf again. I fixed hundreds of systems in '98. I rewrote entire pension systems, entire sale systems, inventory management systems that would have stopped. IT is terrible at this, right? Nobody knows how much is headed off at the pass and how much of that adversary was turned back. Y2K was not a nonevent. We headed off—at least I can tell you in the Pacific Northwest, because I traveled all over and we fixed a lot of stuff. It was pretty simple stuff, there would not have been a lot of trackers sold. You would not have been able to go to Kentucky Fried Chicken and get your mashed potatoes, because those are some companies that we fixed that would have been broken. We do not toot our own horn. We do not run to the next crisis and you do not understand how many holes in the dyke are being patched, and that is a challenge.

Amanda Swenty: Do our panelist have anything else to add to that question?

Maria McClelland: I would agree. It is hard to get everyone to understand that—like I said—until it happens to you. I have been giving these briefings for years about securing your stuff and until it happened to me, it really did not sink in because we spend all of our time defending. One of the things that I am trying to get Kris and our legal team to bless off on is having us do a real phishing campaign exercise, which I've done for my other position and it basically will send out targeted phishing email to whatever you like. You click on that and up pops ransomware. We did it with jigsaw and you would be surprised how much attention we got as soon as the ransomware popped up on their screen and said all of your files are encrypted, you have just lost all of your data, please pay this. That got their attention. Just having something that does not really affect anyone—until it happens to them, they do not really pay attention. I would say yeah, it is still one of those cry wolf, cybersecurity is always so paranoid, they are telling us the world is gonna crash and the sky is falling. Well it is, but like Kris said, we are holding it up. We need help doing that and the only way to do that is the end user. We have got to have everyone involved and keep them part of this whole fight, because everyone has a critical piece in it. You all have access. If you are an end user, you have just as much hand on the door as any of the rest of us do, we are just closer inside.

Amanda Swenty: What we would like to do is sort of summarize some of the wonderful conversations that we have had in the smaller groups for the benefit of the room as a whole. I think Jennifer and I are going to kick off. One of the interesting conversations that we had was my take away is the discussion about hackback—Whether it is appropriate or a really dumb idea, how many people are looking at this topic, is it a serious look at it? As we discussed there is actually a bill in front of the last congress that is likely to be proposed in the coming congress that will indemnify and permit companies who have been hacked to hack back. So take all of the nightmare scenarios that we have talked about and multiply those times ten because now every IT professional, if this bill were to go into effect, could potentially have the ability to go out and strike back at the person that they *think* has hacked them. It is kind of frightening, is it not?

Jennifer Vincent: I would just say I had a conversation with a CSO that was a victim of hacking, and it was based out of Pittsburg. I think you can go online and find out about it, but he was so angry about it, and this has been awhile back, but his initial response was, "I want to hack back, let's go get them." The FBI agent that was there said I have a gun, sit down. Ultimately they did find out who was the culprit behind it, they were from China never to be seen again. They have orders to extradite them if they ever find them. I do not think they ever will. But anyway I just think it is a horrible idea. I get the idea but I think the chaos would be insane.

Amanda Swenty: So Kris what was your take away from your group?

Kris Torgerson: I think one of the more valuable discussions we had was the idea about trying to bridge the gap socially or from a messaging standpoint between IT and the broader business case. The critical role that for lack of a better term, the adults in the room can bring when some tech person starts wheezing on about something that nobody in the room understands. There is value in there. We may not like the message, but if we can grab them and slow them down—the story I relayed is, I was a young security professional in a big company, and the general counsel stopped the board meeting and told me to dumb down the message because nobody understood what I was saying and he thought it was important. If he had not done that, we would have made a bad decision. I would have put the company in a position to make a bad decision because I had lost them. I think people skills, especially of your cyber leadership and privacy leadership, there is a translation problem. We throw out acronyms as if they are water to everybody. Make sure the cyber folks, the IT folks can communicate. You have got to stop them right there. There is a reason why Gilbert cartoons exist and those people are IT folks.

India Vincent: One of our conversations kind of started with that same topic, but switched over to the side of communicating with the programmers who are creating this code. There is also a need for them to understand the security risk and sometimes that means the security group communicating back to the programmers, particularly in the software development field. It may make your code less efficient. It may not run the way you want it to. You may have to adapt and make some changes, but security is important enough that you have to incorporate that into the code. The customers who are going to be purchasing your software want to see that there. I think it goes to a point of separation between IT and security that the objectives are different even though they are both working with technology.

Kris Torgerson: If you do not mind. I was talking to one of my development leads recently and I hate it but I am going to throw out an acronym really quick. I asked my development lead what OWASP is. That is essentially a standards organization that exists for free to help developers write a secure code. My development lead had never heard of it. None of my development staff had ever heard of it. You have got a lot of people that start with the company, and somebody mentioned longevity. I have some people with thirty to forty years of longevity and they have not invested in that sort of mindset. It is important for the risk professionals to push on that because if your IT is homegrown and your CIO is homegrown, starting with security in mind is antithetical to IT in some cases. Your custom developer, that is not the first thing they think about.

Jason Asbury: Our group basically had a discussion about experiences and what we are seeing. I think it is really important for you guys as practitioners out there to have conversations with folks who might know a little bit more about what is happening than you might hear about, day in and day out. Right now, I would rattle off probably one hundred different incidents that I have seen and experienced and out of those hundred I bet five of them went public. There are a lot of experiences out there that people have that you could learn from to be able to educate yourself and your organization, and I would encourage you to do that. To your point earlier about developers and security, think about your organization. I can think of a lot of clients who got some code written twenty years ago maybe thirty, sometimes forty, and I promise you that code is not secure. Think about that in your organization. Ask those kinds of questions. I would just encourage you, reach out and find a network of individuals who can share information with you. I think that is really missing in the risk management world. There is not enough sharing of experience for people to learn from. We just hear about the big stuff, we do not hear about—for every big one you hear about, there is probably one hundred small ones that have happened.

Amanda Swenty: Great. Please join me in thanking our panel for sharing their expertise.