**Project Completed by:**

**EDUCAUSE**

**ELive: Understanding Cyber Insurance**

**June 14, 2018**

**1:00 PM – 2:00 PM Eastern Time**

EDUCAUSE

14 June 2018

>> Valerie: Welcome to EDUCAUSE Live! Everyone. This is Valerie Vogel, Senior Manager of the Cybersecurity Program at EDUCAUSE and I'll be your moderator for today's ELive webinar. This event is brought to you in partnership with URMIA, the University Risk Management and Insurance Association. We would like to thank Mindtree for the sponsor ship of the 2018 EDUCAUSE Live! webinars. Mindtree helps education institutions engage constituents with richer experiences, empower educators, and optimize operations. You are probably familiar with the interface for our webinar, but here are a few reminders. We hope you'll join us in making this session interactive. Use the chat box on the left to submit questions, share resources and comments. If you're tweeting, please use the tag #EDULIVE, that's E-D-U-L-I-V-E. If you have any audio issues, click on the link in the lower left-hand corner. And, at any time you can direct a private message to “Technical Help” by clicking in the top right corner of the Chat Pod. A drop-down menu will appear where you can select “Start Chat With” and “Hosts.” The session recording and slides will be archived later today on the EDUCAUSE Live! Website. Our webinar today is Understanding Cyber Insurance. Higher education interest in cyber insurance continues to grow in response to high-profile data breaches making headline news. Today, coverage exists for a variety of potential losses and liability caused by cyber risk, yet the market is evolving and nonstandard. Today we will learn more about cyber insurance: What it is, what it covers, and how to incorporate it into your institutional risk management and information security practices. We are delighted to be joined by three guest speakers today. Courtney Davis Curtis, the Director of Risk Management at the University of Chicago, Brian Kelly, the Chief Information Security Officer at Quinnipiac University and Robert Parisi, the Managing Director and Cyber Product Leader at Marsh LLC. During today's webinar, our speakers will discuss what cyber insurance is, cyber insurance procurement and governance, operationalizing cyber insurance within your information security program, as well as what happens if or when there is a breach. We'll also have time to answer any questions from participants at the end of the presentation. Please be sure to submit your questions in the chat throughout the session so we can be sure to address them. And with that, let's begin. Bob, I believe you'll be speaking first.

>> Bob, make sure to unmute your audio.

>> Robert: I apologize. So, I guess I just lost my credential as a cyber leader. What I thought we would do today is go through a quick primer and what cyber insurance is and we will get into more of the details. Let's start with what are cyber risks? That term is often overused. When we are talking about cyber risks, we are talking about two things. We are talking about the risk caused by technology being used in your day-to-day operations really at every level and every aspect of what we do. We are also talking about handling and collecting and storing confidential information. Whether it is payment cards, healthcare information, whether it's the variety of new aspects of the private information as defined by the recent EUDGPR. All that results in potential cyber risk. Higher education probably has it more and more varied way than many other industries. But let's talk about cyber insurance and what that is. When a company engages in a cyber breach, the first aspect of cyber insurance they encounter is what is referred to as crisis management or event response expenses. These are the out-of-pocket expenses that accompany or educational institution incurs to deal with an event. It starts with a law firm to help you understand what is going on, legal obligations, hiring a firm to deal into what was the breach, what information was lost. It includes expenses associated with complying with regulations, sending out notices, providing credit, monitoring credit freezes as well as public relations to help you get the message out to the to put elements of the cyber crisis management and event response outside the limits of the insurance coverage. What that means is that while you get the full benefit of the coverage for crisis management, it doesn't erode your overall policy limit. That is a nice benefit we have seen with several carriers. They also have the ability to deal with crisis management and event response in two ways. One is they will provide you access to their panel of vendors. These are top notch law firms and the best of class I.T. forensic companies as well as allowing you to use your own vendors and your own law firms. So, let's assume you have gone through the crisis management. You've had the event and unfortunately someone decides to point a finger at you and say that you caused them some harm. There is two types of liability insurance you have. And liability insurance is one of two types of coverage out there. Liability insurance covers you for harm you cause to third parties. What it amounts to is it will cover you and provide a defense for any claim made against you and it will indemnify you for damages you are held liable for. The two you find in cyber insurance are network security liability. What this is the probably best described as you get infected with a virus or piece of malware and you transmit the virus to the third party, causing them to have harm or suffer from financial loss. They look around to why their systems are down and they realize it was your fault. You sent them malware. They make a claim against you, cyber insurance responds, providing you a defense to that claim as well as indemnifying you for any payment you had to make to that individual or entity. Probably the more popular or certainly the piece of cyber insurance that gets more attention is privacy liability. This is liability to third parties as a result of the disclosure of confidential information collected or handled by the educational institution or information being held under your care, custody or control. This includes coverage or potential lien where you give that information to a vendor. This is what is referenced to vicarious liability. Entities will use lite cloud providers, other entities to store or hold their information. And it might not be the educational institution that loses the data. It might be its vendor. Under privacy liability, the carriers don't make a distinction. If you were the one that took the information in, they are going to protect you whether you lost it or whether your vendor lost it. So, the other aspect of cyber insurance is what's referred to as direct loss. And these are out-of-pocket expenses that you either incur because of an event or they are losses that you actually suffer because you got hit not necessarily impacting someone else. One of the things we have seen with cyber insurance and cyber events that you are often facing a regulator before you ever face a civil plaintiff or claimant. Cyber insurance will provide coverage for legal expenses associated with representation in connection with the regulatory investigation and in some instances, they will also indemnify you for any fines or penalties as long as it is not insurable in the state you are in. This has been particularly helpful to companies while they may have had a breach that didn't harm anyone, they still trigger either a regulation or some statute that has caused them to have to actually do something. Having the ability to have someone help you through that regulatory quagmire often avoids a lot of potential liability coming back to haunt you later on. The next two coverages, network business interruption and data as special teams protections are the losses an institution would suffer itself. These are property-based coverages and deal with that loss of income or that loss of revenue associated with having something happen to your technology. Cyber interruption covers that loss of revenue and the extra expense associated with dealing with the problem from two distinct perils. The first is if you have that failure of security and it impacts your businesses, causes some element of loss and you have to incur extra expense to operate. It will also cover if there's a simple failure of technology not associated with the security failure. If your technology just doesn't work, as long as it is not from a physical event. If you roll out a new piece of software, new application to your system and you can't function the way you anticipated that is potentially covered. If someone backhoes through the power line, that is not covered. That is something you would look to a normal property policy for. Under data asset protection, this is the recovery of cost and expenses your institution would incur to restore, recreate or recollect your data or other intangible assets. What we have seen is higher education probably more so than many other industries has at its core a substantial amount of information. If that's destroyed, corrupted, either because of malware, it is going to be cost associated with recovering the data and recreating it. The policies will cover that under the data asset protection insuring clause. Wrapping it up, cyber extortion which we have seen many ways, situations where people say I have access to your data or the ability to get into your system, pay me some Bitcoin and I will basically make it go away, the policies will cause a potentially covered loss. Whether it is the potential to cause business interruption, to release private information. Doesn't matter. I thought I would put that cyber insurance in a little context for you in terms of growth. Prior to 2011, there was less than 10% -- and just as full disclosure, these are numbers associated with Marsh & McLennan. As you can see from the graph, while all industries grew in terms of their uptake of the insurance, higher education grew faster than MOST other industries to the point now where we are looking at almost 50% of our higher education clients have now continues into 2018.

>> Courtney: Thank you, Bob and our first polling question is up now. If you could take a moment to complete that. This question is do you understand your cyber insurance program well enough to articulate it? As I look at the responses that we are starting to receive, it appears that perhaps most of you are in the category of maybe. We hope through today's presentation you will gain a little bit of insight and have a different perspective on the insurance program and how you may be able to articulate it to others. This tees up the next section that we will start to speak to with regards to understanding the insurance program as well as the procurement and governance. One of the aspects of understanding your cyber insurance program is understanding the coverage itself. However, you really want to underscore the importance of unique exposures and associated risks at your respective institution. The landscape may be broader than what may be obvious in terms of the institutional data pertaining to employees, students and alumni. You want to take into consideration patients, research or other third parties or a vendor who has access to your data or service. Data is often categorized as personal health or other personal identifiable information. It they be governed by laws like HIPAA or specific to laws to the state you are in. This context is useful and provides for a holistic approach to understanding cyber insurance as well as the risk profile of your organization. I find that my institution questions really arise from others with regards to cyber insurance, security and privacy, which are commonly at the forefront of the institution's risk profile which is uniform across other industries as well. Perhaps these are questions that come even from the board level given their broad mix at most institutions. Additionally, I found over the last few years that cyber insurance becomes a major point of negotiations and not limited to maintains of insurance by third parties or your institution but how the risk transfer looks. It is used in some instances to limit the liability of third parties which I find difficult to negotiate. With regards to coverage in particular, what is important for a breach, there may be other services or resources that your insurer may be able to afford you which we will also speak to further in the next section. We are now going to take another poll. And this question is in regards to your engagement of I.T. leadership for the procurement of your insurance program. Do you include them in your process? Yes, no or unsure. This is wonderful. It looks like about 70% or more of you do engage your I.T. leadership in your cyber insurance renewal. I found this to be more than beneficial in my own institution. I can't express how imperative that it has been towards the success of our renewal. But in addition to having engagement with your information security officer, it is also important that you understand who your broker partner is that you are engaging with as well. As you may learn through this webinar, there's many nuances to cyber insurance and having a broker that has expertise in the coverage may aid in gaining favorable results as well. To that end, the combination of your I.T. leadership and your broker for procurement of coverage is paramount. I don't know about you, but other than completing the name of the insured and address, there's not much I can add value to without the help of I.T. leadership. And really, depending on which insurer you are with or which market you are considering for your program, there may be multiple applications to address the various risks and exposures of your insurance program. I encourage you to start that process as early as possible which will help in the long run for others to complete it as well as your brokers to negotiate with the markets on your behalf. As with many other coverages that you have with your insurance program, having discussions and building the relationships via conference calls or meetings with the insurers who will help with negotiations and their understanding of your risk profile. It is important that you add to your institution beyond what may be seen in the application itself and including I.T. leadership in this overall process, especially advocating on their behalf may be beneficial for all parties. It really starts from the beginning of the insurance renewable process in terms of articulating the terms and conditions of coverage to your I.T. leadership as well as setting your expectations for the renewal, understanding what the market is and including when to make changes in the insurer or with the coverage itself. Once quotes received or options received is also recommended. We utilize different resources and benchmarking tools which may come from different sources whether that is from your peer or broker. Your I.T. leadership may have their own sources of information as well and combining those resources may help you to make a more informed decision. Also when there's a positive outcome, you really want to share in that win with your I.T. leadership, indicating to them how their involvement helped to drive coverage enhancement or perhaps minimize increases that you may see in future years' renewal. Also celebrating that to indicate that it is an inclusive process and that you are not making decisions or recommendations with regards to your insurance program in a bubble. Especially if you have to seek authorization or approval from someone else within the organization. Having that feedback and support will really help to solidify the recommendation that you're making. Other key considerations with regards to the procurement and governance of your insurance program really pertains to the area of recharges or allocating a clause. No one said this coverage was cheap, but it definitely has value in the terms of protection it provide from a liability perspective but also in response with the services it allows you to provide when necessary. Many units and departments within your organization that may be able to share in the cost of that risk as well as with the cost of insurance. And having one of these processes in place may help so that others are able to appreciate the cost of the insurance program overall and the risk that they bring to the institutions. Engaging your leadership from an I.T. perspective as well as with your brokers, I think there's a lot of different lessons that you can learn throughout the process of going through your insurance renewal. And through those efforts you may inform your risk organization whether you have enterprise with management or specific topics that come up in a board meeting and using these lessons learned may help to identify ways to further mitigate those risks at your institution. For me, I could not do this process without my broker or engaging the I.T. leadership. It's been a process that we have improved upon each year. And through those as I stated before, those wins are shared amongst the organization gaining in confidence in the overall program itself.

>> We have poll three pulled up and I think Brian, maybe you were going to cover this one or I'm happy to go over that one.

>> Brian: Sorry. Absolutely. I would like to use that as a segue. I think the poll numbers are interesting. Short of not sure and no. So, it's a really great way to sort of move into my area of kind of how do you take advantage of some of these pre-breach services within the policies. So, for us here in Connecticut in the northeast, we have experienced tornados. Unsettling spring weather. Not something that we are typically used to or worry about from a weather perspective. There's lots of homeowners looking at their insurance policies for wind and tree damage. Typically, that's the mindset when we think of insurance from a customer perspective. It is the questions of are we covered and how do we file a claim. What I would like to spend a few minutes discussing is the pre-breach services that Robert mentioned sort of falls generally under that category of crisis management and event response. And what we're doing and what we see as an initiative within these policies I believe that cyber insurance has the ability to sort of move that cybersecurity needle in a positive direction. You think of the safe driver's discount analogy. We can take advantage of the services to help us prepare for a breach that make us a better insurance risk and may ultimately help us avoid having that breach in the first place as well as services we would take advantage of or engage in after something has happened. If we think of these in context of the cyber insurance framework's core, the core of identify, protect, detect, respond and recover, we can use these pre-breach capabilities or capabilities or services within the policy to help us in those areas. If we think about identifying and protecting our assets, it helps us with governance and policy and becomes the planning and the templates that are sort of useful in our written information security plans in those discussions that we are having with senior leadership. They provide value and we can get that from the external sources. Robert mentioned generally with the policy of access to the vendors that carriers provide. You can engage in a very high level. We look at respond and recover. Generally we all have either external counsel or maybe an office of general counsel at our institutions. But these are generally broad scope attorneys that focus on many areas of legal and may lack the focus on cyber incidents to be able to have a conversation and understand what is happening before, what are the things that we need to think about are important. Certainly interesting we talk about detection. Services under that technical and forensic, you may think forensics is generally post mortem or after something has happened. But engaging early and using some of these services you could have the discussion around in the event of a breach, what type of logs are we going to need. It helps prep some scenarios as far as what is happening on your end points, what visibility do you have inside your environment. Really sort of helping you prepare. Lastly sort of that recover capability that we talk about call centers and plans and the ability to stand up that post-breach. These are all things that help inform your incident response plans and build these in certainly before the event has occurred. One of the things that I think Robert mentioned, rather, it is important to think about this concept of a breach coach. We still use the term breach coach. I think coach would be more appropriate in that the concept as a coach is there to prepare you for the game. Not just shows up at the time of the game. What we tend to look at is that preparation. That aspect of the coach and the preparation as a SEO or security professional. You have a sense or you think you know what you know. And having that conversation with the coach, they may show you areas of weakness. They may show you things you hadn't thought about. They offer an external view of your program, of your strengths, weaknesses and threats to that program. And establishing that dialogue before there's a breach is important. They are helping you sort of prepare, discuss areas of focus. You can sort of think of that as a scouting report. So, it's really important to sort of engage that coach well before there's a breach. As soon as you have got a policy in hand, go ahead and reach out to the coach. Start that conversation and start getting value to your programs. I clicked the wrong slide. I also fail as a cyber presenter. Awareness resources. Within the policy there's a multitude of awareness resources, things we take for granted that you may already have in your organization. You may think we are already doing this. We already have a program. But with limited staff and resources, it is just another way for us to help sort of keep information security or cybersecurity top of mind at every level. We get roll based whether it is someone in the finance office, we can get tailored product through our policy that sort of augment our policy or awareness program, rather, which is important in that we don't have a dedicated staff. We don't have teams of people running awareness. Any resource with can get to help move that forward was huge. Sort of my closing slide, my last slide sort of to think through is this concept of cyber insurance as a force multiplier. What it has done in our organization help sort of build structure on our incident response plans and our teams. It has provided policy guidance and reference. It's really enhanced our cyber posture, our cyber hygiene. It has helped to move that conversation as Courtney talked about, moving the conversation and cyber risk to a senior level, to board level. Having the annual renewals, having that dialogue has been important. That is a pre-breach benefit of the policy. While we haven't had to file a claim, and I feel like I might have just jinxed us, we certainly feel we have received value from our policy and support from those carriers in having the policy. Not something we have taken in and put on a shelf and we don't refer to and don't use. I think if you have a policy and you haven't as the poll indicated really taken advantage of some of these pre-breach services, certainly as a take-away from today, go back and relook at the policies, engage in the carriers and see what you can bring out of your policies that would help you operationalize that policy into your programs and your cybersecurity role. I think that moves us to our fourth poly.

>> Yeah. Thanks, Brian. I'm actually going to -- I know we said we would hold questions until the end. But there were a few that popped up and since they are specific to what you are talking about, I'm hoping we can go through the questions. The policy had pulled up about have you experienced a breach. Feel free to respond to that and we will move on to the next section of this presentation. We will start with the first question from Nathan Phillips. Did your cyber insurance provider assist with any prevention planning that you mentioned?

>> Brian: Yeah. Whether it is templates or table top exercises or policy frameworks, absolutely. And we've had a couple of different carriers over the years and they have both had those capabilities as part of the policy.

>> Thanks. And then Brennan is asking has an insurance provider participated in response table top exercises?

>> Brian: They have provided content for those exercises.

>> Thanks. And Nathan had another question about breach coach. Is that significantly different from an outside security assessment like a GAP analysis?

>> Brian: It depends. A posture review is similar to the GAP analysis or risk assessment. The coach is sort of a point of contact within that organization that is more of a holistic view of your program, asking questions around the data that you have, how you collect. So, more of that coach GAP analysis. I guess it depends and a little of both.

>> Robert: Yeah. This is Bob. When you hear cyber insurance talk about a breach coach they are talking about a law firm that helps manage the process. If you think about a patient advocate in healthcare, it might be a nurse or healthcare professional. But they are not the person treating you. They are the person helping you manage through the process. That's a good way to look at the breach coaches that cyber insurance carriers will provide.

>> Thanks for jumping in, Bob. I think that's all helpful. And Jared is asking is data mapping advisable and do you recommend retaining an external firm?

>> Brian: I would say yes, you can't protect what you don't know you have. I think having that data mapping either prior to having a policy or as you renew would important to both your institution and the carrier.

>> Thanks. Alan is asking do you think we could hire a coach on retainer and not bother with insurance? Brian, you are welcome to answer. But Bob or Courtney feel free to add to that.

>> Brian: As the individual on the call -- in the insurance business I think for us organizationally having all of that wrapped into the policy was a lot cleaner for us. Not having to go out and have someone on retainer, not having to have those independent entities built into our incident response plans, having that built into the process was cleaner, easier for us from a cost perspective a little bit. Easier from a budget perspective. But I think individual results may vary and it depends on your institution.

>> Robert: This is Bob. I would echo what Brian said. As a broker, I'm never going to tell someone not to buy insurance. But you can engage with vendor individually. You can engage with a breach coach individually. The thing about accessing it through your coverage is you are often getting a much discounted rate than you would get as an individual consumer and not to mention the fact there's also the insurance that's wrapped around it that will fund part of that activity.

>> I do some additional questions popping up here. But I want to make sure that we have time for Bob and Courtney to go through the rest of what they will be talking about. They might address some of these questions. But we promise to return to them after the next section. So, I think Bob you were going to take it from here after the fourth poll, question?

>> Robert: Sure. We wanted to give you a sense of how a simplified or a simple or sample breach might occur. This is not meant to be dispositive. Everyone can be different. They tend to follow certain patterns. There's the discovery of the event. What we have found is that historically most institutions do not self-discover the event. They will often hear about it either from a trading partner telling them that hey, we just got hacked and you were the person that sent us the email. More unfortunate is when you have law enforcement knocking on your door, telling you that they just found all the credit cards from your site. They found all the healthcare data from your clinic or they found you as the last single point of contact or common point of contact resulting from a major hack. Once you have that discovery, though, there's certain things that are fairly standard. One is to investigate. That first response is key, is critical. Going through and figuring out what happened. Really investigate, investigate, investigate. And make sure that as you're looking down the road against the potential for lawsuit, that that investigation is conducted in coordination with the law firm, the breach coach, to maintain whatever privilege or confidentiality you can. Once you have figured out what happened, that's when you start dealing with how you will respond. If it's healthcare data, you can look at the HIPAA statutes as well as the state breach statutes regarding what kind of notification needs to be made. If it's large enough, you may be able to do it through just a public discussion. But more often than not, you're going to have to deal with impacted parties, individual parties. And then the question becomes what is the appropriate remedial service. You don't want to give credit monitoring to a company that just lost healthcare data. You want to make it also relevant to what happened. If you think it's a lot of smoke and no fire after a forensic but you have triggered one of the statutes, you can offer a variety of things from a call center that acts as triage and figure out what remedy is best deployed. But if you know that something really bad happened and you are dealing with parties who are about to be negatively impacted because of something that you're responsible for, you want to make sure that the remedy is sufficiently robust. Now, all of that is also occurring in the context of being able to make a claim against your cyber insurance. And they will cover the forensic investigation, the legal defense if the claim happens, the breach response? You face a regulator and you often will because they will be right on the heels of law enforcement and coming shortly thereafter are the plaintiffs. But it is important to get that aspect or that period of the response correct because it does impact what happens next. What you can have is if you are the poster child for the poor handling of a breach, it will impact the trust level that individuals have with you. And while higher education might not be as susceptible to income loss, certainly reputation is a huge issue for higher education universities. You will face regulatory fines and penalties if it's determined that you've mishandled and haven't taken the appropriate steps. Or if you have been less than honest or disingenuous. Frankly at the end you can also face significant litigation if enough people are involved or impacted, there will be a plaintiff's attorney that will find a way to certify a class against you. So, I'm going to keep on going, Courtney, unless you have anything to add.

>> Courtney: No. I think you have definitely covered it and what is highlighted in the next couple of slides just simplify some of the information of what you have just shared and the need to engage parties both internally and externally with regards to response. Really no matter how large or small the event may be.

>> Robert: I couldn't agree more. I think what's important to note is if you have bought the insurance, you want to be able to make full use of it. Especially if you bought insurance that comes with that full breach response package. You don't want to find yourself fairly far down the road only to realize that you lost the opportunity to take advantage of the outside forensic investigators, the breach coach. These are folks that handle breeches every day, 24/7. So, while this may be a true catastrophe or crisis for you and no one will ever minimize that, you want to be able to talk to the professionals that are doing this on a daily basis. You don't want to try and handle it yourself. Really this is the time to bring in the professionals and make sure you understand what is going on before you start talking to outside parties. The last thing you want to do, because we have seen it on several situations, is attempts to get out in front of the news before you have the facts. And you really often will cause more harm than good if you try and go that route. So, I think we've also talked about what's going on when you have a breach. One of the things that drove the purchase, or the rise of cyber insurance was things like the duties that were imposed by various state, fed and now international laws and regulations that required very specific type of notification. Several laws now are in place that require not just notification, but the offering of a remedy. Whether it's credit monitoring or credit freeze or some other activity. You also want to be having a little bit down the road. You want to be able to make sure you are appropriately dealing with the event as it is right now. But this is not going to end when you send out that notice and offer credit monitoring. This will have future implications. How you handle the event will determine how long a horizon this event has. Does it dissipate and be done within the next couple of months or are people still talking about it a year later and you are still in the press and utilized in a presentation like we're talking about today as how not to deal with a breach. So, I think we are done with our slides.

>> I think you are right, Bob. Thank you and thanks Courtney and Brian as well. I think we will just start going through the some of the questions I have seen here in the chat space. Please feel free to keep adding questions if you have thought of anymore. I'm just going to briefly call out a few resources that might be useful. In coordination with URMIA we updated and republished the liability insurance. And EDUCAUSE we have a library page that gathers all these cyber insurance related resources in one place. Feel free to bookmark those links and check them out later. I will go back up to a question from Phil that said if your coverage includes coverage with notification or credit insurance for the individuals whose information might have been taken, who decides if it is required or advisable if an institution were to decide to provide notification to the students would the cost be covered? Going to let anyone, Bob or Courtney or Brian.

>> Robert: This is Bob. I'm not Dodging the question but it does depend on the coverage. Several carriers will allow for what's described as voluntary notification. As long as you can show that the information was potentially impacted, most, if not all of the carriers will allow for notification. The thought being that if you don't notify that one group, they will be treated or viewed as treated in a prejudicial fashion. So, policies will typically err on the side of caution and allow for that voluntary notification. The question becomes do you want to make a notification if you don't have a need to? Sending someone a letter that you lost their information is not always the most wonderful thing for someone to receive. So, you kind of have to decide are we -- you can certainly offer credit monitoring to someone as a voluntary benefit. But I don't know that I have had any clients that will decide to make a notice when they have absolutely no reason to do so other than for public relations. Typically they will notify and provide the ability for people to reach out to them. But the individual notices are usually tied to some perception that there's some obligation to do something.

>> Thanks, Bob. I will move on to another question about forensic analysis. Should an institution establish a relationship prior to a breach or after the event?

>> Brian: I can answer. I think absolutely before the event is critical and whether that's on your own or through a retainer with an independent forensic vendor or through a vendor your carrier recommends as part of the policy. Having that relationship ahead of time, having that in your play book or incident response team is important, or incident response plan. So when you need them you are not making first introductions at that point.

>> How might you go about finding a forensic investigator or firm to work with? Do you tend to look to your peers for suggestions?

>> Brian: Absolutely. Certainly within EDUCAUSE there's a great community of peers that you can turn to and then I think also for us that forensic community is a fairly small list of vendors and we've over the last few years used the recommended vendor from our carrier within our policy.

>> Great. Thanks. How about -- we are going to talk about actual payment of ransom ware covers or the ransom itself?

>> Robert: I will take it as an insurance question. Every claim is going to be subject to unique facts and circumstances. But ransom ware and malware, those payments have been covered and are covered typically under a cyber insurance policy. They have tended to be small. Send us 300 Bitcoin or something like that. But they are covered.

>> Thanks. Should universities ask specifically for coverage of GDPR violations or would that be covered as standard say yes. GDPR went live a couple of weeks ago at the end of May. It's still a little unsettled as to how the regulation will be interpreted. I think universities, especially universities that attracts students and faculty and staff from Europe will potentially be impacted. It doesn't matter that you are domiciled in the U.S. If you interact with an EU citizen and have information referred to as data subject, you are subject to that regulation. I would say yes. You certainly want to ask for the coverage. Even if you don't have coverage that says GDPR specifically in it, most privacy components of a cyber policy will pick up a significant amount of the harm or the liability that running afoul of GDPR can cause. The issue becomes -- GDPR has certain components to it that are new and unique. Things like the right to be forgotten, the unfortunate chance that you can run afoul of the regulation. Not because you have hurt anyone but just because you haven't followed its strictures. It has broadened what has deemed to be confidential or private information, you want to ask about GDPR and there are several carriers offering a broadened privacy cover that would pick up these new GDPR exposures.

>> Thanks, Bob. Another question is can our mistakes our own risk decisions reduce the amount of monetary support provided? If they have a vulnerability that an institution knows about and haven't been able to address and that is exploited, would that invalidate the coverage?

>> Robert: Not necessarily. The carriers ask certain questions and they require a submission. Typically they will ask you questions and map their application to the framework which is just a way of looking at and bundling questions around information security. As long as you haven't misrepresented yourself, it should not have an implication on whether or not coverage is paid or not. Around certainly, there's no expectation by the carriers that everyone is perfect. They understand that things can happen. Where you might run afoul of them and where coverage might be negatively impacted is that if you know you have a breach and don't tell them about it until after or you know you have been exploited. But again, they don't expect anyone to be perfect. They understand that things happen. They understand that people deploy software that may have to be updated. That is not something they will hold against an insured.

>> Thanks, Bob. I appreciate that.

[Audio cutting in and out] [Audio difficulties] [Please stand by]

>> Looks like the majority of that audio clip -- for participants who are able to hear us, we are just checking to see if we can resolve this audio issue to make for a clear broadcast for all participants.

>> Valerie, you can continue. We will continue troubleshooting to make sure the audio is nice and clear.

>> Thanks, Adam. I didn't know if you wanted to add for to what you were saying, Brian.

>> Brian: I would just thank you for posting in the chat window the resources that EDUCAUSE has for those budget conscious communities. It's a great resource. Whether you have insurance or not, go check that resource out because it will help you with your budget.

>> Courtney: This is Courtney. I would add maybe quantify what your risk is by taking a look at your profile and identifying -- there's also information readily available that pertains to breach and liability and notification and response. So, if you are looking at a worst-case scenario they may be able to ascertain whether an insurance premium is wanted against what a catastrophe breach may be.

>> Robert: I would add, no one is suggesting insurance is an alternative to good risk management and maintaining kind of good digital hygiene. The point really is that at some point, additional piece of technology and additional protocol is not going to completely reduce the risk. It is at that point you look at do I need a million, do I need five million of insurance. But it is always part of a larger risk management effort. As much as I hate to say this, the insurance comes after Brian and Courtney have done their job in making sure that insurance comes into play.

>> Thank you all for chiming in on that question. You might have an answer for this one. Is there any trend of institution requiring vendors to store information whether it is employees’ student information carry their own cyber insurance?

>> Courtney: I can take this one. I see there's another question regarding deciding how much insurance is acceptable. Where possible we do have technology errors and omission or cyber insurance as a required line item of coverage. We kind of use [indiscernible] to determine what that amount of coverage should be. Whether that company has access to [indiscernible]. And what type of data that need be. You want to look at the risk of what that vendor may have access to and make a determination whether it is a million, three million or more of coverage that they should maintain.

>> Thanks, Courtney. Appreciate that. This answer may vary. But are institutions required to notify students in accordance with the laws of the state which they come from?

>> Robert: Yeah. It doesn't matter where the college is. It matters whose information they lost. So, you might be in New York but you have all students from Connecticut. You have to follow the Connecticut laws in terms of notifying those individuals. And if you have individuals from New Jersey, it's those. You don't follow -- you don't necessarily -- you're not going to base your notification on where you are, but you base it on the laws associated with [indiscernible]. The people whose information you lost.

>> That makes sense. Thanks. I know we had a couple of questions we were going to try to get to. I apologize for the technology difficulty we had here at the end. But I want to go ahead and wrap up this session.

>> Valerie: On behalf of EDUCAUSE, URMIA, and our speakers, this is Valerie Vogel, and I thank all of you for joining us today for an engaging session and conversation. Before you sign off today, please click on the session evaluation link, which you will find in the bottom left corner of your screen. Your comments are very important to us. The session will be archived on the EDUCAUSE Live! Website, including slides and a complete replay. Please feel free to share it with your colleagues. And finally, please join us for the next Elive! Webinar on Thursday, July 12th at 1:00 p.m. Eastern to hear about Transforming Education with a Data-First and Cloud-First Approach. On behalf of EDUCAUSE, this is Valerie Vogel, thanks for joining us today for EDUCAUSE Live!

[End of webinar]