Project Completed by:

EDUCAUSE
Exploring the 2021 Information Security Horizon Report
Thursday, March 04, 2021
1:00PM - 2:00PM Eastern
>> Welcome to today’s EDUCAUSE Webinar: Exploring the 2021 Information Security Horizon Report. This is Jamie Reeves, Portfolio Manager of Communities & Research at EDUCAUSE, and I’ll be your moderator for today’s event. EDUCAUSE is pleased to welcome today’s speakers: D. Christopher Brooks, Brian Kelly, and Mark McCormack. I will introduce them in just a moment, but first let me give a brief Orientation on our session’s learning environment. If you’re tweeting, please use the #EDUCAUSEwebinar. We hope you’ll join us in making this session interactive. To open the chat, click on the chat icon at the bottom of the presentation window. You can use the chat to make comments, share Resources, or to pose questions to our presenters. Be sure to select “Panelists and Attendees” from the drop down menu to engage with everyone. We will hold Q&A until the end of the Presentation; but we encourage you to type your questions into the chat throughout the Webinar. If you have any technical issues, please direct a private message by selecting “Panelists” in the Chat dropdown.

The session recording and slides now let’s take a look at the poll results. It looks like about a third of you have read bits and pieces. Another third of you have some work to do right after this webinar to go ahead and start reading it. We have about 14% are wondering what Horizon Report is. For those who have not had a chance to read the report you can find a link in the chat. The session recording and slides will be archived later today on the EDUCAUSE website. And now, let’s turn to today’s presentation. This webinar will explore the trends, challenges, panel of global experts and the 2021 Information Horizon Report. Members will height trends and challenges how each meeting its many information security challenges capitalizing on opportunities. Thank you all for joining us here today. With that, let's begin.

>> Good afternoon. I want to talk about what we do with Horizon Report. So a large part of what the EDUCAUSE Horizon Report team does is to engage in sense making of the thoughts, ideas and data that we collect from the expert panel. The 50 members of this year's group all first time Horizon Report panelist with an eye to representation of different context, gender, ethnicity size and type. We collect data and generate conversations about key trends, technologies and practice that is will be important of shaping the future in higher education. One of the guiding principles to producing our series is from this quote from Dennis Gabor that emphasizes the possible futures. It is one that moves us beyond a narrow problematic and potential incorrect exercise of prediction to one that is more diverse and open ended and thinking about futures in the plural.
Predictions are often very shaky ground. For one, they tend to be based on a single feature. A prediction will happen next year. Recall if you will the prediction by Bill Gates. The predictions can rob us of our agency and ability to shape future. If we think X will happen because it has been predirection. If we think of the future as something that can be invented we regain that agency. We can exert and influence what will happen. An array of possible futures. In this way the question shifts from what will if future be to what future do we want to or might we have. The principles were outlined in this article for thinking like a futurist. This was one of our most popular pieces we produced here. So what are these five principles that guide us? Forgot about predictions. Predictions tend to focus on a single event and hinder us social economic and political trends and a potential transformation. Second focus on the signals. We don't have future about the future only about past. As the situation becomes different and become to recognize the normal patterns are beginning to change. Our experiences with the pandemic should be a clear illustration of this. Third, we need to look backwards to identify larger historical patterns so we can consider the possibly futures. We don't repeat history but repeat historical patterns. Fourth, intermitting signals helps us consider the changes of the best way doing things to tomorrow's way of doing thing. A variety of different do mains to carry out this exercise. The information security team was guided by these five principles. To the produce this report. Now I'm going to hand it over to Mark.

>> Thank you, Christopher. Hello I'm Mark McCormack senior director of analytics and research at EDUCAUSE. As Christopher shared the background and the thinking that guided or approach. How did the things shape out? What will you find as you dive into the 2021 Horizon Report? The first thing we asked to do was to reflect the trends out there in the world that they believe are going to shape the future of higher ed information security. By trends we mean those larger macro forces that seem to be moving in a different direction. And we didn't want to panelist discussions to focus just on new technological trends or just on trends taking shape within higher ed specifically because we know those are the areas panelist discussions naturally focus. We wanted to focus on the broader landscape. So we did ask them to talk technological trends. We had them vote on the trends that are important in each of those categories. This is how their vote shook out. The first thing I want you to notice we identified what we call an uber trend. Panel list discussions kept coming around to this trend of remote work. And that's not surprising. With so many aspects of our lives including work and school having become remote or virtual or online, you would expect discussions about the future to wrestle with this idea and the possibility that our lives will continue to be remote in some ways. Think about the information security workforce. Might enable institutions to recruit staff. Being remote means taking on new challenges and supporting staff. So remote work can change the makeup of the security workforce itself. It could change the nature of the work information security professionals are called upon to do. We can think having the staff, student working remotely from their homes using their personal devices like some of us may be doing right now presents information security professionals with new challenges and protecting the institutions and those end users. Beyond that uber remote work. You can see those top three trends that the panelist selected for each of those categories that we cover in the report. In the social trend categories our
panel list talked about expectations is going to lag far beyond. They talked about the importance of data privacy as our web of personal devices continues to expand. They discuss the growth of the big tech vendors and the implications of that for things like that contract negotiations. For technological trends. Our panelist focused on the cloud base of end points and networks. The need to plan for routine and security incidences and increase of devices. Under economic trends panelist focus on implications of remote learning or the strain of security, staff, and budgets as they are called to take on new and additional work. They reflected on new opportunities to help identify efficiencies and drive down cost for information security solutions. As institutions explore new business models we can think about the implications about those changes for security units and continuing to protect the institution. I think the environmental category of trends may be the most difficult to think through. Maybe the connections don't seem quite as direct, obvious or some of these things are the front of our thinking. Continued to contend with weather events or the strains of remote work of power infrastructures. We can think about their efforts to protect the institution in those areas as well. Finally, we did even in a year like 2020 we boldly venture in political trend. The spread and weaponization like videos and social media. The implications of national information for monitoring against the threat of bad actors. This is how we summarize. This trend is a thing that is happening. It is observable. We can see things headed in the right direction. This is what the workforce shortage trend is. I won't make you sit here and read the whole thing. You can see in the evidence section we might link to another article or report that might be worth reading. We might highlight something that is happening at a specific institution. There is a lot more here than just a list of the trends. We packed a lot of rich material and wanted to make it worth your time to dive in and observe everything that is in here. After their discussion on the trends. We asked the panelist to identify and vote what they believe are the key technologies or practices that are emerging that will important for shaping the future of higher ed. These may be new technologies or may be practices or technologies that have been around but there may be new develops or taking on a new significance for the future. And these are the top six technologies and practices or panelist identify in no particular order. Cloud vendor management. Managing these relationships will become more important as institutions rely on cloud based services and success in managing those relationships will depend on things assessment of those vendors. We know that end points are one of the biggest areas of vulnerability of the institution. Demand new and cloud based end point institutions. More seamless options. Especially when you consider the number of applications and systems your faculty, staff, and students need to access on a daily basis. End points have implications for data protection. In the future there may be more of a focus on the data themselves. And security professionals will need to explore data techniques among other things. Research security will be an important consideration for institution. Research, of course, an important part of many institutions do. As research becomes more depend on things high performance. Research will become a bigger area of vulnerability. Finally as our students become more and more aware of how and why institutions are using their personal data. Those students will expect the institutions to have the protections in place to use the data safely and responsibly. And this is how we summarize what it means for hire Ed and security. You can see on the right hand side a few exemplars like you see here at University of California Berkeley. A way not only illustrating
what it might look like as the ground. And we provide that second box that popped up with each practice a few bits of data that show how the panelist along some important dimensions that we asked about. How costly it would be to implement. For the degree to which that practice can help the institution in addressing issues equity and inclusion. The risk it will succeed or fail at the institution and the overall impact on the institution information security. Finally, we pack a long with each practice a few suggested readings should the reader want to continue to explore that even further beyond the horizon report. With that I'm going to hand the mic over to Christopher. Christopher?

>> Thank you, Mark. While the future cannot be predicted alternative predictions the Horizon Report team offered four scenarios what higher education might look like in the next ten years. These scenarios where not simply made out of thin air they were in forms of trends, signals, technologies, and practices identified by the Horizon Report panelist. In addition to the constraints of being use only data available to us, we will we constrained by models of the future. We used four to help us envision future. The growth scenario current trends continuing in the future with minimal disruption. Adopts a guiding value and governs behavior. Paints a picture of a rapid break down current systems and infrastructure. Envisions a society of systems that have been phenomenally changed. In this way the horizon reports team here engaged in a science fiction of information security. And finally we explore the implications of everything that we found and consider how they should inform plans for the future. We ask some members to identify the most important two or three implications for their own higher education context and discuss how those implications play out there. The report includes seven essays versus range of perspectives. U.S. we have two non U.S. higher education systems. We have one industry perspective as well as vendor perspective. Some of the implications.

>> The future doesn't happen overnight. The planning happened almost a year ago. With an expert panel convening way back in July of 2020. This would not have been possible with Jamie, Mark and so many that were involved in the sense making and coordination or as I like to call it putting a puzzle together. Our expert panel can be found at the end of the report. Many are on the call today. Thank you. These experts are colleagues. They are peers, they are friends. I'm going to highlight some of those essays as Christopher pointed out. We will jump to the next slide. This one in this report generally more generally in our community we look for shared experiences and like to learn from one another. Adaptive and comprehensive approaches to the security of our information systems. For speaks to the scale of our systems and networks. Her essay will be familiar to systems across the country. And speaking of moving across the country. Our next essay author is in California. We move from Connecticut to California. Reflect on the global impact on U.S. research institutions how we maintain the collaboration on the context of a number of challenges. Rereminds us that our primary challenge make sure are tuned to the influences of society at large. I want to thank Mike for his leadership and supporting EDUCAUSE, the cybersecurity program. There are a number that Mark and Christopher have discussed. I will highlight a few here. We didn't mention the sponsors or the submitters. If any of you have follow up questions for any of these exemplars please let me know and I'll put you in
contact. Let's start with Stoney Brook. Challenge end users a serious of increasingly sophisticated fake phishing attempts. Kansas state university requirements from the federal government for safeguarding CUI. Rise was developed to meet that need. That was developed by Ian. The University of Michigan. The ViziBLUE provides transparency for students. Simon Fraser systems that support not only web applications but services such as data center and VPN. What else on the horizon? There is more on the horizon. We have more. Solar weeks next week. Our conference coming up later in June this year. I'll turn it back over to Jamie and we can go over to Q&A.

>> Great. Thanks Brian, thanks Christopher, thanks Mark. I want to encourage panelist to go ahead and type in any questions you might have for the team. We can start from the top here. Brian, when will the next Horizon Report be published?

>> The next Horizon Report I believe is teaching and learning Horizon Report will be provided in April. We have not decided the publishing date.

>> Fantastic. Folks should look for that to be hot off the presses. The April 26th should be launch date. We have another question. Do you see a trend of regional or other collaborations among multiple institutions to strength their security posture in changing and growing threat?

>> That's a good question. I'll take that one from the top. We collaborate with a number of other institutions in the U.S. we are working with our partners in August and others that was an author. We are seeing the collaboration. We talk about borderless networks. The threats of the attackers know there is no international boundaries for those. What we are seeing is some collaboration with security operation centers. There is a little bit more of that happening. I'll let Mark and Christopher add.

>> I was going to invite folks take a look at the scenarios. Within I want to say each of them we painted some interested way in which we forecasted and predicted the future in which different types of even across sectors might actually pay out. Just some interesting ideas.

>> In terms terms across collaboration the places where I noted that emerging out of our panelist discussion tended to be either in areas of thinking about ways to leverage that collective bargaining power and negotiating contracts or going out on the market that there is a benefit there and a collective, collaborative approach. The second area is thinking about standardized practices or approaches that a collective collaborative body could help develop for the field. So I think those are some areas of potential for collaboration that our panelist identified.

>> That's great. Thank you Mark. We got another question. Given the width of your interaction what did you consider note worthy of this year's report?

>> Who wants to go first?
>> I think the remote work. I think that uber trend was the most note worthy.

>> I agree. I think Brian within that finding and we call it out here and there in the report. There is a huge element to all of this that maybe is exaggerated when you think about the remote work. The remote works of learning. That the awareness and the practices and behaviors of that end user, that human end user of the device or network that that is becoming it has always been important. I feel like the report environment is bringing that in the sharper relief. And so as a question for security professionals to think about what are the needs that emerging to train, to raise awareness to support and prepare those end users to protect and security their devices and networks as they do their work.

>> I would suggest as an extension or perhaps cuts into that the focus that we had on student privacy and student data. That's increasingly becoming an object of concern. Not only people in the information security space but higher education at large. We have seen some recent data that suggests students are very aware of and concerned about the ways data is being collected and used and oftentimes they don't have a lot of confidence in how the institution is doing that. I think that is something that we are going to definitely see is becoming more important and requiring policies and attention in the next few years.

>> That's great. Thank you. We have another question. It is around COVID funding. Can you give ideas how to use the Horizon Report to tie the information security needs to the potential round of COVID funding?

>> I'll jump in first. Thinking about the different sections and features of the report. I want to highlight the peer based elements. There are a lot of examples to link to or connect peer institutions. Maybe there is emerging practice or someone exploring or innovating. I think there is opportunity within the report to learn more about what your peers are doing and connect with them as a place to start and think about future planning and where your institution can go from here.

>> Great. Thank you, Mark. Do you have any advice for under resourced institution for the 20% enrollment decline?

>> We did publish the cybersecurity. Published budget conscious guidance. I can find that link and I will make sure I will share that. I make sure I will ask the person so they can have it as a resource so they can refer to.

>> Great. Does the report show products and metrics?

>> I don't know we had metrics directly related. I don't know we had that data directly in the report.
If I'm understanding it correctly we didn't evaluate specific products. I know there are other resources we have across EDUCAUSE that might help beyond that Horizon Report. Obviously for someone that comes to me is our data service. I know we have other tools in your area as well Brian.

Absolutely. I'm taking notes for all the referrals. They are in the resources. We do have some of that.

That's great. Thank you. Many institutions are limiting their technology offerings. Do you have any advice for one institution to maintain environment while ensuring safety and ease and two individual faculties how to navigate the new institutional restrictions related to technology?

My gut is we are trying to do everything we can to not impede collaboration because it is so important. How we are going to continue to advocate for that collaboration. Understand how some of those streamlining is limiting or impeding the collaboration. I think that is a good follow up conversation.

And then we have another question around the roll of insurance providers. What role do they play?

We are in the process of rewriting. We had done FAQ a few years back and it is in the process of being updated right now. I live my entire time in Connecticut. We had an individual that was famous for his automobile safety initiatives back in the late '60s and what that impact on insurance industry was. Is their analogy to cyber? Cyber policies would be written. There was no validation that you had any of the controls in place. You might have done a one or two page questionnaire. I think being more makes us ecosystem. We can do a whole different webinar. To some degree cyber insurance is fuelling paying for that ransomware. I'm happy to take it offline and follow up.

Great. Thank you, Brian. We have a question. Does the report what is the uptake?

I don't have metrics in front of me. We have well over 125 institutions that have told us. They are listed on the EDUCAUSE site. Some of those large names you recognize. I do think we reference it once or twice within the horizon report. I think the Berkeley exemplar.

That's right. We highlight the exemplar in the cloud vintage management and how the University of California Berkeley is using that tool.

Thank you. We have another question around some future thinking. What are your thoughts on the persist tense of virtual education? Do you believe it will change around online curriculum? Is this a threat to the brick and mortar institutions?
I'm going to assume that the question in terms of information security. We certainly played with a few scenarios about thinking about the impact of the pandemic moving students into virtual environments and the increase I think Mark referenced that when he was looking at the trends as it was related to the increase points of places we have to protect. I think for sure there are implications there if online remains a large portion of higher education continues to do. The degree to it is a threat to the brick and mortar institutions that depends on the degree to which higher ed can think about ways for lack of a better the opportunities created by the pandemic into something that allows them to transform themselves. What they have achieved in the past year in terms of moving online. An attempt to predominately face to face institution. So I think there are a range of possibilities there. A lot of that will depend on factors as well as individual institutions of decision making.

I think that covers. I hope it answers the perspective we were coming at. I did see in the comments. A comment that said one of the big takeaways talking to the institutions was key to building and maintaining my slide just moved. That collaborative nature what we do in the cybersecurity program. Connecting and collecting those dots across the country, across the globe. That is where it comes in talking and interacting with each other.

I think the spirit of the horizon report is that tool to be able to use to talk with and collaborate with your colleagues and peers. It is a great conversation starter. And as well as a wealth of information. So another question it looks like one of our last ones is this a topic you will follow in the next few years? I assume from Horizon Report perspective.

I certainly hope so. Personally information security. I think we will follow along with privacy. As Christopher has said really see a growth and focus as well. We may go that direction as well.

Yeah, and I'm sorry I don't remember if we covered this at the top of the webinar. Historically the Horizon Reports have been teaching and learning purpose. This security report is the first instance of us expanding the horizon series outside of the teaching and learning boundaries. It is very exciting and new and different for those reasons. We do have plans to continue to expand the horizon series outside of just teaching and learning although we will be maintaining the teaching and learning Horizon Reports as well.

I don't see any other questions in chat. And key technology developments.

On behalf of EDUCAUSE and our speakers, this is Jamie Reeves, 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 Chat window. Your comments are very important to us. The session’s recording and presentation slides will be posted to the event site. Please feel free to share these resources with your colleagues. And finally, please join
us for the next EDUCAUSE webinar on March 30 to hear about “Machine Learning’s Growing Role in Research.” On behalf of EDUCAUSE, thanks for joining us for today.