EDUCAUSE
EDUCAUSE Live! - Influencing a Security Culture:
From Community College to Ivy League
Tuesday, October 8, 2019
1:00PM – 2:00PM Eastern
Welcome to EDUCAUSE Live! This is Brian Kelly Director of the EDUCAUSE Cybersecurity Program, and I’ll be your moderator for today’s ELive webinar. We’d like to thank Quest for their sponsorship of the 2019 EDUCAUSE Live! webinars. Quest is the go-to solution that helps universities and schools better move, manage, and secure their Microsoft infrastructure. You might be familiar with the interface for our webinar, but here are a few reminders. We hope you’ll join us in making this session interactive. If you’re tweeting, please use the hashtag EDULIVE. That’s E-D-U-L-I-V-E. Use the chat window on the left side to make comments, share resources, or to pose questions to our presenters. 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 audio issues, click on the link in the lower left-hand corner of the screen. And, at any time you can direct a private message to “Technical Help” by clicking in the top-right corner of the Chat window. 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, and available on the EDUCAUSE Live! website. Our webinar today is Influencing a Security Culture: From Community College to Ivy League. Oh no, not another security awareness session! While the answer to that is yes, this will not be your typical session on security awareness. You'll hear ideas and solutions to engage your community, no matter your institution's size, Carnegie designation, or public or private status. The presenters believe in this mission and have witnessed great success in their awareness journeys that will be of benefit to all. Sure, they are both from New Jersey but don't hold that against them. We are delighted to be joined by Trisha Clay, Chief Information Officer at Hudson County Community College. Trisha is a strategic Information Technology leader specializing in infrastructure and applications support management, project management, collaboration, and information security. She has a Master’s of Business Administration with a Project Management concentration from DeSales University and is a member of the EDUCAUSE HEISC Awareness and Training Community Group. We are also joined by David Sherry, Chief Information Security Officer for Princeton University. David leads the Information Security Office, which has responsibility for security, architecture, engineering, operations, risk assessment, compliance, business continuity, disaster recovery, and awareness and training. David has over 25 years in information technology, with the last 19 solely focused on security, and has led security missions in several verticals before arriving in higher education eleven years ago. He has an MBA and two security certifications and is an active participant in the nationwide higher ed security discussion. David and his wife,
lifelong residents of New England, moved to the Princeton area in 2016, and he’s working hard to teach his staff the Boston accent. Thanks to both Trisha and David for joining us here today. And with that, let’s begin. David, over to you.

>> Thank you, Brian, very much for that. Welcome to our website. "Influencing a Security Culture: From Community College to Ivy League." You are not stuck in a time warp. We actually presented this at the last conference in Chicago earlier this year and we'd love to reprise it today and share it with you. Thanks to everybody who has participated in the poll. We are seeing somewhat of a bell curve from three people who have been doing National Cybersecurity Awareness month from 2004 to 11 people who have never heard about it so happy to be able to explain it to you. Those in the middle who have been doing it several years or recently started it. Lots of good information coming out of it. Our two campuses have been doing national cybersecurity awareness month with you. We're happy to shower our results with you. I'm David Sherry.

>> I'm Patricia Clay.

>> I'm from Pennslyvania.

>> And I’m from Massachusetts. We're transplants to the garden state. We hope you come visit us sometime and enjoy what the jersey shore and what the rest of jersey has to offer.

>> So Hudson County Community College is in beautiful downtown jersey city, New Jersey with a campus in unity. As you can see from the arrow we're right in the middle of the United States. People in California will probably argue with with that. At least we're in the center of the urban area in New York City, it's hustle and bustle. Our campus does not look anything like Princeton, which is where you are.

>> Yes. Princeton is located in the central part. It's interesting, the people will say the great thing about principles son is we're located halfway between New York City and Philadelphia, but the worst part is we're located between New York City and Philadelphia as well-meaning we compete for resources against those amazing cities and all that he have this offer in terms of technology. Here we are, both from New Jersey, and happy to share some of our experience with you.

>> So we have two very different schools. Hudson County Community College is a very different institution, two-year with associate degrees. We serve 15,000 students a year that includes continuing education, a large participation of college students and not native English speakers and immigrants.

>> Much different from Princeton, which is a total 100% residential college ranked in one of the top polls in the United States that you can find. Happy to announce this morning we have
received our fifth Nobel prize in my short 3-1/2 years here so much different from what you'd expect in Jersey City in Hudson County Community College. The interesting thing is as I sit here from a CISO at a university, Pennsylvania is a CIO, we share one goal, to make a result cultural aspect of our campus. It doesn't matter if we're residential, four-year private, whether we're traditional, non-traditional student inner city college. Our one goal is to make security a cultural aspect of everything we do on campus. It's even built into the mission statement I have with my group, which you can see here. It's to make security programmatic and cultural. Programmatic meaning it's plugged into everything that we can possibly plug into at the university, from hiring someone, to someone unfortunately being let go or retiring, from a transfer, to purchasing a new copy machine, to signing a contract with a local firm, to a new hosting facility. Anything. If we can get into the security aspect of it as early in the game as we possibly can and make it programmatic, security will increase and risk decrease. And then making it cultural. Having a group of seven people as part of my team. Seven people cannot be everywhere on this university, but if we can have the entire university, no matter what your role is from working in the bake shop to the president and everyone in between understand that in the era that we live in, in the environment and the vertical relive in, that security is their job, once again, security increases, risk decreases. That enables our group to participate in the mission of the university, which is to increase teaching, very search and learning. Programmatic and cultural. You'll hear that result really thing -- result really thing throughout the next 45 minutes. The most important word to take away from today.

>> So one way to influence your campus is through security awareness. So that is -- it's October. It's National Cybersecurity Awareness month, and we want to bring that security awareness not only across the country, we want to bring it into the camp for students, faculty staff, and I look at even though we're the its department, it's still our job to educate people and a big part of that is information security. Now we have a question for you all. Security washes. Do you think it's worth it. There's been a lot of conversation about this. If we have just the best security tools, maybe we don't need anybody to really understand information security.

>> You're right. Yes. And the work that is time, effort, resources, tools, it could be a lot. Most people say no. There's a lot of research that says awareness doesn't have as big an impact as the tools do, but look at our audience. We are amongst friends. My goodness.

>> Thank you all for being here.

>> Yeah. Only 2% so far say no. One person.

>> We don't call you out.

>> It's somebody from my staff making sure we have the data, right. I'll have to call them out of that. We would expect that from you, folks, anyway. Taking an hour out of your day. 83 people participating, probably more that will be listening to it at another time. Of course, we think it's
worth it. Pennsylvania and I agree, but. Thank you. As of this particular research, 95% of cyber -
- successful cybersecurity tax were the results of a phishing scam. If you work on any campus
this is the bains of your existence. 70%, the security risks are reduced 70% when you're investing
in cybersecurity training. He we put that in the forefront, that really can make the difference. It's
the human vector of falling for that one phishing scam or that business account compromise that
can really start the house of cards falling over.

>> Another quick poll. Tell us about your security awareness program. Do you have some basic
training, mostly online training? Wow, look at that.

>> A mix

>> David: The highest one is mixture of online training. That is awesome. That is the hallmark
of a mature program

>> Patricia: Right. Get to them in the beginning, the middle.

>> David: less than 10% are saying that they have really nothing going on.

>> David: Maybe that is why you're all here. You do have a budget and you need some more
ideas.

>> Patricia: So y'all have a budget. Do you need some ideas? Is that why you're here today?

>> David: All right, why don't we end that poll. Looks like we've got some good numbers there.
Still under 10%. That's no budget, no resources, no awareness. All right, can we move actually
off of that poll? We're going to jump into another poll as well. How is it working

>> Patricia: Yeah, how is your security program working. Do you consider it to be a success?
We've got some -- respond to us in the chat box. I see some people sawing they're in the right
direction, but need new ideas. We want to strengthen our effort. Some say not yet. With one
thing I'll say, sometimes you just need to get started. We'll talk about that as we go on.
Sometimes you feel like you're shouting in the wilderness perhaps. I started doing this at a
different institution where we started with National Cybersecurity Awareness month. Sometimes
you just have to get the ball rolling

>> David: I've seen some of the comments in the chat are awesome. Much more effort than ideas
than we appreciate. They're getting tired of hearing from us. We'll talk about understanding the
community you're dealing with and changing things up and maybe coming up with interesting
thus as well. At Princeton we're blessed to have a full-time security and awareness program
manager who it's, sleeps, drinks, and breathings security awareness. Creativity, lots of events,
lots of online things. We'll talk about that more as we go on. Looks like my slides have gone all
the way back to the beginning. If you'll bear with me we'll catch up to where we were. Thank you for all that so far. It looks like we have a good range of people who have been doing this awhile, who have plenty of in their program, and people who are looking for interesting points where they can get better and we'll talk about that. Once again, we want to go back to the word "culture." It's really all about your culture. Culture at Patricia's school is much different than at mine. When we went to the Educause security conference, they were seven or 800 people there last time, we get people in their itself group, people are small itself groups, large itself groups, a whole awareness training idea. It really is all about the culture. What is their view of security in the first place. Do they think it's useless, overrated, are you considered the department of no, no, or know, know. Temperature working on a college campus we have subcultures. We have the student culture, staff culture, fact actuality -- culture. Knowing how to impact those is one of the key things we want to bring you today, so it's all about the culture

>> Patricia: So, what is culture? It's the social behavior and norms in an organization or people. We want people to be in the position for security to just happen so that like David said, we're not the facility of no, because everybody has begun to realize it's seeing in that that personally identifiable information has to be proprietyed, that their account is important. And it obviously is important to them, but it's not only important to them, it's important to the school, the college in my case, or it could be the cunning education department. It's important across the whole campus. So we want to get that baked in and have that be a parted of just the social behavior and norm, so what are the barriers. I hear this all the time. Not from my team necessarily, but we can't get them to think about that, we don't have the time, we don't have a dedicated security person, it's not going to have any value. Wait, that's not my job. I'm just the technician. You guys respond in the chat. Other barriers to a security culture you've heard of. What are those things you've heard. What I started to do when I was new with my team, my team was to let them know hey, this is all of our job, it's a part of all of our job. And when I talk to the executives and other campus leaders, we start talking about that right as we're doing it. As David said, when you're bringing people onboard, but new technology and talking about hey, how is this going to be -- is this secure and bring that into the conversation at the beginning. So here are some more -- that is SANS research, right? Who are Bahr 81st to security culture and who are supporters. Some of these things might surprise you and maybe they don't. Probably depends where you work, right. Information security. Yeah, information security is onboard with this, right

>> David: Of course.

>> Patricia: Sometimes they're looking at operations. It's 50/50. If you've worked operationally in technical, you know -- Tech, you know there's a tension there. You can bring the culture aboard, move the yellow or orange bars down and keep pushing there's blue bars over. Make it a part of all of our culture. So hey, time for another poll. Describe your institution's security culture

>> David: I could tell you if the Princeton team was on and they would be answering it they
would probably give me some smart-alec comments that has a Boston accent to it. I say that because they did that in Chicago. Describe your security culture. Take a minute and put it in the chat window. As you can tell, we believe in this culture aspect. It's interesting, a lot of charter on security avenues over the last couple of days because a non-U.S. university released a report on a breach that they had, an incident report. A pretty in-depth and transparent look at a breach that occurred to them in 2018 into 2019. The interesting thing was re-recognized after doing the incident response was that one of their weaknesses was they needed to change the university's information security culture. They said their information security program had to be more strategic and had to place more awareness on security awareness and culture. They said culture a few times in that paragraph. I said this is great. I wish I could go up there and offer any assistance that I possibly could because we really feel that in an ever changing population, students transfer over -- change over 25% each year, having that can you remember from the time they walk in to the time they walk out is extremely important.

>> Having them learn as they go through however lounge they are. We have them two or three years. I saw someone commented that some people think that the technology should solve everything, that you don't need the security washes. One of the things I have a lot of conversation with executive leaders are there are people out that it's their whole job to break things, break in to steal our information. We're playing a game of catch-up in that that is all they do and we have other things we need to be doing. We need to be indicating students, we need to be having that research. In a community college, we need to have that impact on the local community

>> David: Lots of cool comments going by on the chat. Most of it teams to be positive, from the president on down, trustees on down. Really, really good. Seems like everybody is going in the right direction. At the same time it's like we all have a lot to learn from each other, shared resources is a good thing for us to be thinking about. We just had quite a bit go through the chat about challenges. Does anybody have a horror story they would like to share really quickly? That you had any horror stories, Patricia?

>> Patricia: I had a little bit of a horror story. We had somebody leave the security department that had let's say important information that should be safeguarded and when the person departed, we found out that they had very secure information held in a very insecure way.

>> David: 2019 Red Sox. Well played, Brian Kelly

>> Patricia: oh, my goodness, that is poking where it hurts. You probably have run into these things, too. You walk into someone's office and they have a question not related to information security and they were like oh, I was emailing my tax forms and your eyes get real big, and that's when you know you may have a little more work to do with that person in their information security, their awareness

>> David: I'm sure if we let this go a little bit longer we would have lost or stolen laptops that
were not encrypted and. People traveling with devices, areas or pockets that had RDP turned on. A whole host of areas. Horror stories from a technology perspective, a people perspective and Prosper spec. We've all had them. Coming together as a shared sculpt and sharing success stories as well as horror stories is an awesome thing. Stolen devices and password sharing. Oh, my goodness. How can we exert influence? I have been at Princeton just over 3-1/2 years and one of the things I had to learn really quickly was the existing culture. And I could tell you the existing culture would not have been ready for me to come from Massachusetts and start implementing mandatory, mandatory, mandatory, mandatory. We had to develop a reputation, a reputation as being a partner, a reputation for people who rolled things out thoughtfully, reputation as a department that did not hinder any business or security process, but securely enabled it and that's what we were working on. An email server under the desk. Thank you, Sarah Curtis, we can pass on those. We can spend at least the next half-hour talking about that. How can we influence that?

>> Patricia: David was talking about what it was like at Princeton before he arrived. At Hudson it's a two year school. We have a lot of mat lated students who are going to go on. We also have our continuing education department it is our mission to serve the local community. I don't have resident students to plug into. I used to previously doors the residence halls. We don't have residence halls. I was talking to David before we came on I'm looking forward to our new student center opening because that gives us a nice wide open area where we can do check-ins, privacy check-ins and things like that where I don't have a venue for that right now. So I can't pretend we're Princeton and we're residential and neither would David and Princeton want to act as though they were a community college

>> David: Right. So, you know, thinking about the culture, because we work in university setting, it's all different cultures. We have the students. They think differently, they act differently. We have to really address them differently than we do the faculty. Princeton exists because of the faculty not the other way around. We are just an avenue for them to get their reaching and recertification done. And then we have staff. Staff we have a little more influence on, direct influence. It's more like almost a corporate culture. We can tell them exactly -- what they need to do to get their job done. It's understanding that culture, knowing the message has to be different. Talking about Princeton is just rolling out a password manager. We have to make people wear of that depending on the population. The students will use it differently than the faculty. Same thing with general knowledge about being safe at home. Maybe the students don't want to learn about that, but the staff has more interest in it. So consultedy understanding the different populations and understanding them is one of the most important steps to begin with. A key strategy, when we were rolling things out, we do not say no. I don't think the word "no," is in my job description. I am here to help Princeton expand on teaching and very search and learning. Security office, they say no, we can't do that as a reputation or we can't do that, that won't work. We say yes, and. That will create a separate thing for you. Why don't we do more access control or use a password manager. We don't always have to come in and say we're right. We look it when we present something to a customer, they can have input in. As soon as they ask us to change or modify one little thing we have a buy in 100%. Sometimes we don't get all we want,
but we know that at the minimum we have a certain minimum-security standard that we would have to rely upon and the university has come to expect that from us

>> Patricia: Right. I think it's key, David said something there about being strategic. I think being a partner where it's yes, and. Yes, you need to accomplish something, and we need to secure the data. How do we do that together. So we have awareness events, right. Traditional message with a twist, right? Some of this is going to depend on your culture, like we said. Some of it is going to depend on your budget and what kind of -- if you're a team of one, you can't be everywhere. But you can do brown bags. We have had some great success with that. We've also recorded some of our talks, so they can be played back later. Finding a event time at a community college is difficult. Internal job affairs. It's a technical job fair. You're talking about hey, information security, whether you're there to get hired, you're good. Branding logos and give aways, David's team has got the bomb with this. I love the tiger.

>> And students love lap took stickers. Oh, my goodness.

>> The game-changer is to get in front of the key influencers. This year I had the opportunity to get in fronted of the faculty organization. I had four minutes; I was two minutes longer than the dean. And I actually had people come up and ask me questions about password managers afterwards, so I know it's making a difference

>> David: Certainly. If you can get a few key faculty on your side, we work hard to make sure the computer science faculty is with us. I was telling Patricia before we went on that over the next two days my team will be at what we call flu fest. The entire Princeton community can come through and get their flu shot and there's a few tables can go to afterwards, one of them being ours. They can protect their physical health and protect their online health. I'll talk about the fun we have. We'll get in front of thousands and thousands at the Princeton community the next couple days and we're excited about that. So remember, everybody learns differently so just how you present your curriculum is a way to influence your culture. We have online presentations that people can watch. We have short videos on our website that people can pop into anytime. We have online classes, in-person classes. We have a Facebook live. We do webinars. We do department meetings. We stand in the student center. We do anything we possibly can to get people where they are. Sometimes they like to come at lunchtime. Sometimes they don't. If you teach them at lunchtime about something about their personal security, whether it's securing their home network, talking to their children about secure use of the internet, privacy and social media, how to prepare for an episode of identity theft, all of a sudden they'll show up. They'll take their hour punch and come learn about something. They love transparency. We have had security incidents that we share with the technical community here. We have done red team engagements and we share the results. We've given them where we have done well and where they could do better. Also, social media. Facebook, Twitter, Snapchat, what's app. Students love that. And Instagram, they love that a little more than Facebook. Remember their social and come at them from different ways as well.
Right. And showing that result makes the difference

David: Absolutely. So you're looking at one of the logos uses. Influence your life, influence your culture. We use this every October for national cybersecurity month and different times as well. People come to expect, understand, and know we're coming at them in a way that can help them in their personal lives. We really feel strongly the someone is thinking about security from 5 a.m. to 8:30 a.m. they'll be thanks from security from 8:30 a.m. to 5:30. You can't turn it on and off. Don't click on a link, don't do this, use VP N. If they do it at home, they'll do it in their Princeton life as well. Think about how you can influence their outside campus community.

Gamification. Here are two of the things we've done in the past. People like to play games and win prizes. Even when they get the question wrong, they like to play. We have had two different episodes of gamification. Cyber world of fortune and corn hole. People wanted to come down and they're that thing spin around and click and possibly win a prize. We've had great engagement, people were laughing, learning. We heard lots of things, I wish my husband or wife knew this stuff. We were giving away power banks and charger kits that had our logo on it. The web cookie corn hole was directed at the students. We had biggest Alex Hawes, digital footprints they leave behind. They got a tick about talking through the student center, people have fun. A win-win for everyone.

Patricia: Sometimes a little dress-up doesn't hurt. People dress up as a fisherman. We have had some success with that in the past. Swedish fish are popular. And don't bite into the budget too much

David: Yes. And some uniqueness. Princeton is blessed right across the start to have an old traditional theater that loves to partner with us. We have had great success in showing security minded or privacy minded events. Some of them at midday, some towards the end of the day, one in the evening. We ran an '80s night showing war games. Some of you may remember that from the '80s. Afterwards we have a panel discussion. What did you think about this, how did it impact your life. How has security changed, how has it not changed. It costs a little bit to do this, but the theater is a terrific partner. They do all the advance work for us for the movie posters and securing the rights for the film, free popcorn and soda. We have a good time with that. Finding ways to impact your culture to a non-traditional method can certainly help you in the long run

Patricia: So finding that theme and you running with it. There is our Swedish fish. The gold top is -- that is different. We borrowed -- we have our Hudson fishbowl too which has been very popular. I actually had a student I talked to on a couple indications for quite a long time who fell for -- and this was a social engineering thing, it was one of those gift card scams. she lost a significant amount of money which was way more than she could stand to lose and she said to me, if there's anyway, that I can make sure that another student doesn't fall for that, and so we have used that as an average. Now we make sure we get in front of students, so they know where to go looking.
Isn't that great? Students like listening to other students. They might not listening to the CISO or CIO. If you can send out things to your graduate students or any body something like that they love learning from each other. Don't take the bait, folks, don't take the bait.

David: Here are some other events that you should consider. Be there for shred day, spring and fall cleanup, be safe at your school. I know for a lot of move in, move out is from on residential campuses. Graduation prep. This is a great one. You're about ready to go out in the world. How are you securing your social media presence, that your perspective employers are going to look at

David: The be safe at in your scale is great. Partner with your public safety, university health services, your police department, with counseling, anything that keeps a person safe in some way. Public transportation. Whatever that you have on your campus. If you can have some kind of fair on your main green, student center and you're part of it, once again, if they just see the security table maybe they'll stop, maybe they won't. If there's a bunch of players where they can get information about safe walk, the blue light phones, how to get back to campus safely at night and the security team is there is a super big impact. Think outside the box how you can partner with other people across the campus just to get the word out

Patricia: We have awareness video cop tests there. If you have a TV film, marketing, communications, majors on your campus, theater is another good one. Students love to put together little movies. One thing, it doesn't have to be long

David: It does not have to be long

Patricia: We want it to be short. So we're passing the awareness message, we're getting people involved, students, and we have a work product that comes out of it

David: Perfect example, I get the opportunity, I had four or five minutes in front of really the high level leadership across the university, a group that gets together twice a semester, 200, maybe 220 people, all leaders across the academic and staff across the campus. I had a four or five-minute info commercial on a password manager and utilizing the power of one our acrossive groups, they wrote a short skit and a crazy little song about password managers and the dangers of it. The people who were there may not have remembered my slides or what I talked about, but they certainly remembered the skit and the song. When I was able to do a follow-up at the next one people were a little disappointed that I didn't have students coming to sing a song. Just remember there's all different ways to get the word out and most important to influence your culture. That is what this is about, plowing your culture to make the security mission that much more in effect.

So as you -- in effective.
You're that little red fish right there and now all the blue fish are following along. If someone asks here how do you know these events and non-traditional methods work. Certainly you could measure it but one of the ways I know it works is people stop me on the street and in the hallway and ask me questions that oh, I didn't think about that, how can I get a password manager at home

David: Exactly. Or we see adoption of our optional security tools. Some of our security tools are mandatory, like putting two factor authentication in systems. Some are optional. We see increases in being invited to department staff meetings. Sometimes we'll give a class on a certain topic and they'll have us come back and talk about other things. We'll go to a staff meeting for give minutes or an hour and talk about anything you want us to talk about or bring whatever mission we want to talk about. The more we get in front of people and they realize these are interesting people, they want to help, the department of know. We had one department call is the defenders of the Princeton universe. They created a logo. This was career services. Think about career services. This is a group of dedicated, passionate, hardworking 24/7 people who want these Princeton students not only to get a job when they graduate, but then support them after the fact. You don't think there's a lot of interaction with the security team, but you know what? We do resume reviews with them, mock interviews, we talk to them about the cybersecurity job. You don't have to be a hard-core geek. You can be a graphic designer and go into security. We speak to them about privacy and the right things to do on social media. This is with career services. So we're getting some staff, some students. Once again, increases the influence on campus. Sometimes you get a cool title and a cool logo as well. The culture can change. One of my staff members and I just did a talk two weeks ago in New York City and we said we can tell the culture is changed. How can you tell? Because when we now want to roll something out, we're seeking people to volunteer to be on a task force sore group, we get overwhelmed. People understand that we're here to help them and we -- see the culture changing as a result.

So the big take-away here, it's important to get started. So we have to just take one event or idea and do it. When I was first starting on a small campus with a really small team and I thought how can we start doing it. We started. We started tweeting, posting on Facebook, started doing that because we could, because we could email the campus. Then it was fishing con text. Take one of these ideas and test it out on campus

David: Yeah. If you'd like you can all type in the chat window happy birthday. In two days from now my group will be three years old. Think about that. Three years old. We are really in our in fan see when you figure our school is 273 years old, we're three years old. So we're going to have a little fun on that -- with that Thursday singing happy birthday to ourselves. We came then and we were doing awareness sessions less than 90 days later. We went from nothing to giving classes. We had the logo, website. We just jumped in. Just get started. We could have said let's think about this for a year, we could have been doing focus groups, we said, no, let's just do it and we have been going strong ever since then. We like to say we went from zero to 60 in
three years. It really has been that moment for us

>> Patricia: So what are you going to take home with you. Respond to us in the chat and has had ideas tickled your brain that you want to take back or take outside the door. You're probably sitting at your desk

>> David: Yeah. Is there something you want us to expand upon, or we can do that. Laptop stickers are cheap, starting a Twitter account is cheap. Starting a table as at an event is cheap. Swedish fish is cheap. Great idea

>> Patricia: And if you have cybersecurity majors on your campus, that is another from one to reach out to them. I have organized with our cybersecurity lead faculty to have the students join in on a webinar to learn more about cybersecurity careers. Sometimes just get in fronts of students and they start talking about things

>> David: We all have smart students. We all have smart students. So shall we start to wrap this up and maybe get to some more Q&A?

>> Patricia: Sure. So our missing is the same no matter what our size, designation, tight or budget. Our institutions could not be more difficult. There's not a right or wrong approach. We're all just trying to get to the same finish line, and that dramatic change is going to come to that culture change

>> David: Think about the mission of my group. It says nothing about technology, nothing about we're going to have the most powerful fire wall and the best ids, architecture. We're going to make security thinking programmatic and culture. That is how important I think it is. I think we have had an extraordinary three years at Princeton, and we have impacted the culture and they're ready for the next steps. The bottom line is start when you can. It's about 10 to two eastern standard time. I would hope by 5 p.m. your local time you'll have an idea that you can be thinking about that you can start at your campus just things we talked about, something new. We would love to hear from you after the fact that things you think of. Start as soon as you can. So keep in touch. Our email addresses. We are both on Twitter. I think we met each other on Twitter because we were both at the security conference and we were tweeting, and we bumped into each other. It's amazing how an online interaction is now we're sitting in a conference room both in New Jersey and here we are talking to our friends and colleagues across the country. We thank you for your time today. We have a few minutes, I'm sure to do some questions and I think Brian will be coming back in to close us up.

>> Thank you so much for this presentation. We have about 10 minutes, so if you have any questions feel free to write them in the chat and we'll get to them. And yes, Brian is going to join us with a few questions coming in that we already have coming in.
As I'm watching the 80 and thinking about the 80 folks that are there and registered, just our community, what Educause and the cybersecurity program you provide, we see names that may be unfamiliar to us in the chat if there's an idea that we can reach out and start conversations and continue those conversations, you said you two met via Twitter, we have met a bunch of new people here today on chat. This community is integral to the success of all of us. Think one of the questions we possessed, you touched on it about how you address how you know you're succeeding with these non-traditional methods. Do you want to elaborate on that a little more?

David: So walking around campus and seeing some of the awareness materials that we have put out, even posters force upcoming events or laptop stickers or Post-it Notes that says do not put your password here, please use the password manager. As we see more and more of that, people are sublimely telling us, all right, we're getting this, we see what you're doing. Our continual and expansive security awareness program, yes, every session that we do we get the 20 usual suspects that will show up anytime because they're either going to gets a piece of pizza or a cookie or whatever. We're getting another department touch point. When we do that we track that. We had one from department A. The next time we had three people from department A. We're getting word of mouth out. Just the adoption rate for people to become early adopters, people who want to be focus groups, people who stopped us to say when are you doing another movie event or thanks for letting me win that power bank at flu fest. We just know it's changing the culture. We can sense it. Is there a message behind it? Hard to do. Metrics are meantime to identify and time to recover. That is what the trustees want. We think we're moving in the right direction.

Patricia: I get a lot of reports of phishing and social engineering not just to me, but to our official reporting mechanisms and more people reporting than used to. I'll get to when we'll be for right now, I can tell because when -- as a CIO, when I'm talking about implementing a new technology, they're asking me about the security not just me asking them, so that really makes a big difference. Faculty saying I didn't think about this before or students or staff, hey, I noticed that students sometimes do x, y, or z that is not secure and that is something we can respond to.

David: Princeton last a process called architecture and security review. It's not mandatory, it's opt in, but it's is the security office doing triage on a possible technology solution, host provider, what have you, we bring together fingerprint key areas from database, networking security, contract. We even talk about the vendor and we become like the middle person, the one they can point the finishing to ask the hard questions, so we don't have to ask the hard questions of the solution provider. Once again, this is voluntary, but demand is outpacing supply. We do it once a week, more often than not two or three times a week and we're looking through January. It's slight the way we have impacted the culture. They come to us to connect off this and we're booked three months in advance. Can't get any better than that. [overlapping speakers]

David: Go ahead.
That was one more question that came in. The question was around if both of you have implemented multiple factor identification, ought case. I would say the awareness campaigns that went around that implementation.

David: so we are all customer groups, faculty staff, grad students, 99.4%. We are have chosen where to put multiple factor authentication in systems, resources. We are at that success rate mainly because of everything else we've done. It was low and slow. We didn't turn it on for everybody at once. We put it on in certain locations. We expanded it. We believe in it once again, because of the reputation that we have built, the influence we have, the partnerships we have. We have been able to implement that broadly

Patricia: And we're just getting started with multiple factor in its. It is something that is critical, but with a small team that is something we're going the start rolling put. It we the goal is to roll it out to everyone. It can have a snowball effect

Patricia: Here is a question, laptop tickers, webcam covers. They are absolutely great. The other thing is you is about adapters, hubs, where you can plug one in. People love that as well.

Alex also said about partnering with communications and marketing. We have definitely done that. They worked with us on banners for the portal. This year we had a press release out that we're National Cybersecurity Awareness champions.

I'm going to pass it over to you, Brian.

I was going so say one of the key things, congratulations on the three-year birthday or anniversary. When people think of Princeton you think, wow, you have a staff, you're not like the staff of one, but really when you got there three years ago you were a staff of one so I think it's important to recognize wherever you start in that journey as we said in the open you can move through that journey, not to waste time, just get started on it right away

David: Thank you, Brian. On behalf of EDUCAUSE and our speakers, this is Brian Kelly, 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 EDUCAUSE Live! website. Please feel free to share it with your colleagues. And finally, please join us for the next Elive! webinar on Wednesday, October 30 from 1:00 - 2:00 p.m. Eastern Time to hear about Budget Fundamentals for the First-Time Manager. On behalf of EDUCAUSE, this is Brian Kelly, thanks for joining us today for EDUCAUSE Live!
End of Webinar