Michelle Norin: My name's Michelle Norin. I'm the Chief Information Officer at the University of Arizona and I'm still catching my breath a little bit. I'll just say a couple things, you know, it's easy to get distracted around here and if you wander too far, it takes a long time to get back. So we had to run *[laughs]*. We were way over on the other side of the – of the place, so welcome to the presentation. This is a presentation on computer data, cracks and leaks and I'm here as the Michelle Norin for a couple of speakers.

Before I kind of venture into our topic, I have an announcement that I need to make to all of you, which says that if you decide to leave and – or when you leave, for the sake of controlling the crowds and kinda who's where, please use the escalators at the north end of the concourse, which I'm not even gonna attempt to point 'cause I don't know which way north is from here.

Audience: Straight out this hallway and ____ the _____.

Michelle Norin: Okay, so out and to the right. Those are the north escalators. Okay, so we're here to talk about information security from a couple of perspectives. I'm the CIO at the University of Arizona but I also wear another hat. I am also the co-chair of an organization under Educause called the Higher Education Information Security Council. Jodie, who's one of the speakers, is also a member of that community and I think what's exciting about today – we have two speakers. We have Michelle Iverson from the Department of Education. She's the Director of Information Assurance Services and we have Jodi-Ann Ito from the University of Hawaii, who is their Information Security Officer. And I think what's important about the arrangement of the speakers is that there is effort afoot to create a partnership and a working relationship to strengthen that relationship between federal student aid areas and the higher ed or Educause community, which is the – usually higher ed but sometimes K through 12 community as well – to work together around information security practices, policies, guidelines and the highest element of Educause is focused on that very thing: providing resources to the higher ed community around security and programs.

It is definitely a trend and has been a trend over the last, I'd say decade, to put more focus around information security. And there's a lot to talk about there but there are a couple of elements that we'll talk about today with regard to this particular topic. One is the notion of prevention and reaction. Preventing situations that might cause compromises with, particularly data and information – protecting information assets. How we prevent, how we protect

those assets. But then if and when there is a situation or a compromise, how you react to it. What are your practices? What are you required to do versus what you may choose to do as an organization. What federal laws are there that require you to take certain actions? What state laws are there that require certain actions? So there's two sides of that equation: preventing, protecting and reacting when there's a situation. So that's one theme.

The other theme that I think is important that are speakers will touch on today is who's responsible for protecting information and most security programs today will tell you that everyone is. Everyone plays a role in protecting information assets whether you're the programmer writing the program to protect the code or whether you're a user who has an ID and a password that you're not supposed to be sharing or whether you're accessing certain kinds of information and systems. Everyone has a role to play in protecting information and so when we talk about an effective security program, one aspect of that is awareness, a creating a mindset and a culture in your organization that truly is pervasive and truly is in a fashion that people – when you say protecting information, most people are gonna understand what that means and what role they actually play in that equation.

So we're gonna hear from two speakers, both from a protecting perspective and from a reacting perspective and then this notion of mindset and culture and so we're gonna start off with Michelle Iverson and she's gonna talk about some of the technical aspects of that equation.

Michelle Iverson: So good afternoon. There's also, for I guess everybody got a seat, so – as Michelle told you, I'm the Chief of Information Assurance and Chief Information Security Officer for the Department of Education. So my office helps write the information assurance policies for the department. We do the compliance and we also do the operational aspects of monitoring and protecting and defending the department's system. So as I thought about data cracks and leaks and one of the things that I think about when – I guess I should make sure I know how to use this. So buttons to push so you get my briefing slides. Here. Yeah, we do IT for a living.

[Laughter]

Male: There's a wireless remote, too.

Michelle Iverson: Okay, great, thanks. Okay and that said, I'm also gonna – so when I started to think about data cracks and leaks, I started to say, "What really are the underlying issues today and where we begin?" And it really comes down to some of the engineering and actually, as we get started – how many of you are on the IT side of the house? So we got a lot and then how many on the business side or the line ops? So about maybe a little under half but a good split and hopefully, my talk will resonate with both communities 'cause you both have a role in this.

So when you look at the pictures up here, that on your left is the Tacoma Narrows Bridge and if anybody knows about the Tacoma Narrows Bridge, it is a – it fell in 1940, due to the harmonic resonance that caused it to shift in the wind and it is a premier case study that is used in structural engineering and it changed the way education about structural engineering was taught during that time. The photograph on the right is a picture of the Kansas City disaster at the Hyatt Regency in about 1980 when there were a bunch – the Hyatt had just opened. There were walkways that collapsed and fell, killing over 115 people. In that particular instance, what had happened is a failure of communication between the initial designers and architects and then the builders of the system where they changed the design mode which left it 30 percent less capable to hold the weight of the structure.

So how does this – can anybody tell me how might this relate do cyber security? Does anybody have any idea? Prevention? The original design had some flaws in it. Okay. Okay, well that's – *[laughs]* flaw against flaw, right? Ensuring flaw against – insuring flaw. That's very good. Any other ideas? Okay. Well, the key thing is a single flaw can topple the entire system. Something so simple as changing just a design for a tie rod with screw bolts that caused 115 deaths. And so those single flaws – it comes down to the engineering and the communication, the original design, the verification and validation of those designs.

Okay, I do wanna go previous. Okay. So when we look at the cyber security landscape, today's landscape is networks upon networks, hierarchies of virtual and physical – it's very hard to know where one networks stops and where another one begins and it's getting more and more prevalent as we get all of the smart, small devices as, you know, PCs almost become obsolete as everybody has their iPads and their iPhones and probably – is there any Dell folks in the room, Androids and other products.

So, as that landscape becomes more and more pervasive, the IT engineering challenges and dangers grow as well. There's a broad spectrum of critical applications and infrastructures and the process control systems that depend on secure and reliable software. Vulnerabilities – everybody knows about patch Tuesday and different vulnerabilities that requires constant due diligence and remediating those vulnerabilities and its estimated that over 90 percent of reported security incidents result from exploits against defects in the design or code of software. So it still comes down, whether it's a software engineering, network engineering – that's where the baseline is of some of our security problems.

So – and just like in structural engineering and other aspects of engineering, a single flaw can topple the entire system but just like with the Tacoma Narrows Bridge, we can learn from it and we can start taking those lessons learned and incorporating those into our designs in the future. So that comes down to building security into the system in the same manner that you would the structural or safety and other types of specialties used needs to be applied when you're developing or designing your own information systems.

The security requirements should be part of developing requirements as you would your business requirements. So as you're talking about a student loan system – or actually we were talking at lunch – will go to a system where parents want to look at grades of their children. So when you're designing that system, you have to start looking at, "Okay, what are my business requirements?" Well the students need to have a login account – well then I'm need to start saying well; "The teachers have to have a login account. Oh gee, I didn't think about it but parents need to have a login account, too." If you didn't think about those requirements up front, you wouldn't have designed that in and now you have the students handing out the passwords to their mom, their dad, and whoever else may need it because we didn't build that into the system. So those security, those access control mechanisms, have to be thought through under the business case when you're developing the business requirements of the system.

And failure to incorporate those results and marginalization of what the security requirements are and how important they are to protecting the privacy information, protecting financial transactions and lots of times then because they're marginalized, when you start doing transfer cost performance and schedule, cost and performance, then security often gets left in the last part of that. And then when you have to add them back in afterwards, when your compliance people come or if you have a security incident,

adding them in after costs a lot more than developing them in the first place when you're doing your business requirements.

Okay, so where do we start? Now, I mentioned over 90 percent of the security flaws come from secure code. And so really a good place to start is with secure coding practices. I put up here to websites – one being the Sans top 25 most dangerous software errors, with that link, which is actually a mitre, which is a federally funded defense research organization and so I listed just the top five of the 25. SQL injection is a means to steal the keys to the kingdom. That really is an attack against your database systems, which there was one statistic I read – and you know, everything's true on the Internet so it must be right – most applications are getting over 70 attacks per hour with these type of SQL injections on up to about 200 per hour, so with automated scripts that are constantly testing the security of your databases.

And then I'll go down cross-site scripting has taken over as the number one vulnerability for computer security. It used to be buffer overflows in coding and now it's cross-site scripting and cross-site scripting is a vulnerability that basically through a website, through their user data that's input, a script can be automatically run that one now exploit the data and allow a malicious attacker to get your – whether it gets your username, your password, your e-mail and other sorts of privacy information about you – and this is because some of the Web developers, as their building your webpages, haven't you secure coding mechanisms. There's especially for Web development, there is the Open Web Application Security Project. It's a great resource – has tools for you to be able to check your websites. It has tools on how to develop secure code. All of it is free so whether you're paying somebody to go develop a webpage for you, ask them to use those tools.

When you go to accept the product, renders tools yourself and if you're building – if you're on the IT side and you're actually building – use these free resources that are available. One thing I didn't put up here is network segmentation – and I'm not going – there are lots of good things you can do to build security into your system but from basic, where do you start for good, solid, security engineering and design, software security practices and then network segmentation. Break your system down into manageable chunks where you can manage the security policy. You control what data is coming in based on that.

Your systems, when and if – they will be under attack at some point – your system should degrade gracefully. It should maintain the security under attack, so as all those people are trying their cross-scripting or a SQL injection attack, that it maintains its security and when it can no longer handle all of maybe the data and it gets overloaded, then it's gonna fail in a secure mode.

And then continuously monitor for vulnerabilities and threats activities. One of the things that we have under an ONB mandate that we are working right now on department systems is the continuous monitoring program. With that, there's automated protocols now – the Security Content Automation Protocol– put out by NIST, many of the vendors have adopted these security protocols. Microsoft has lots of tools and many of you are probably using Microsoft's tools, both in their network management and their clients to be able to give you these protocols to tell whether your systems are vulnerable or not vulnerable.one of the key things is knowing what's on your network. You can't defend, you can't secure what you don't know so it's very important to put some of the Security Content Automation Protocol's tools to have them report that there on your network and what their configuration status is and that can all be automated at this point.

You've got to identify where your sensitive data is. Your intrusion detection response teams, if they get a notice that Server X has been compromised, if they don't know that, "Gee, that's everybody's social security number in the university," or, "That has all of my financial transaction data for the last five years," there's a difference between responding to that and a webpage that says what's going on Friday night at the social club on campus, right? So you gotta know where your sensitive data is, where the crown jewels are. Conduct near real-time automation and then develop a robust threat analysis and security awareness program. Continually ask yourself, "Who's after my data? Why would they want it?" And a lot of times, you know what – and I came out of Department of Defense before I came to the Department of Education and it is a little bit different culture.

[Laughter]

So but I was the first one to go, "Oh, who would want Department of Education data?" And when I got here, I'm going, "Wow. We have a lot of responsibility to the American public. Maybe even as big as the Department of Defense." Because we do have our children's data. We do have our citizens data from – all the way from, you know, preschool on up through and beyond postgraduate

school, especially when you start looking at tracking student loans and everything well into adulthood. And then just the amount of financial transactions and the amount of data or money that is being passed and tracked and stored. So, you know, my hat is off to the challenge of everyone in this audience. It is a tough job and it's an important job.

So please keep thinking about who would want your data, where are they gonna get it, could they take a piece of data from the system and a piece of data from that system to actually make a bigger picture? Because you really want to know how would somebody go about targeting me. So that's important.

By using integrated systems security engineering we can build safer systems and we can minimize data cracks and leaks in the future and protect that PII and protect the financial transaction data that you all are responsible for.so with that, I'm gonna turn it over to Jodi Ito from the University of Hawaii and she's gonna talk about the actual protecting the information as I've talked about protecting the systems.

Jodi-Ann Ito: Thank you very much, Michelle, and thank you all for being here after lunch. This is a tough slot and I applaud you for being here. Thank you very much. And by the way, this is Michelle's contact information. Write it down, memorize it. She'll be a good reference for you. So I am here – I'm sorry, this isn't the right slides. There's two sets of slides, so let's see. They had actually linked both the first slide presentations together and then tomorrow, there's another person coming in in the afternoon session. So my slides aren't here? They have the other set of slides for tomorrow's person.

No. This one? We'll try this one. Okay. No. Sorry. Keep talking. I have a jump drive that has it on it, though. Should I grab it? Yeah.

Michelle Norin: You can talk and I'll look.

Jodi-Ann Ito: Apologies.so how many of you printed out my presentation, then? No. Okay, so I can wing it and you guys will never know. So basically, what I'm here to talk about is as an institution, what should happen to you after that is a breach, so that is basically why I'm here; however, so the things my attorney said I could talk about. Yes, the University of Hawaii has had a data breach. In fact, more than one and yes, we are the defendants in a class-action lawsuit that has not yet been resolved. Okay, so that's what my

attorney said I can talk about. So everything else will not be about, specifically, the University of Hawaii but with that said, I do have some experience in this area and so the way I wanted to frame today's discussions is that there are a lot of bad people out there. The cyber criminals out there are out to get our information. They can monetize it and basically, some of the statistics I've heard is that the global drug industry is about $600 billion, okay, global drug industry, and compare that with the global cybercrime industry. That's about $500 billion, so they really want our information very, very badly.

Now, with that said, why do they want our information? Because they can use it for financial fraud. The other thing they wanna do is to take control over your computers, because your computers, as you use them what do you do with them? You access sensitive information, right? You log into your account with your passwords. If they can gain control over your desktop computer, they can put a software on your computer called keystroke loggers that record every single thing that you type, including accounts and passwords. That then allows them to get into the systems legitimately. So this is a huge thing and a lot of these types of incidents cannot be detected. We call this advanced persistent threats or cyber espionage. They don't want to be found, so they're very good at hiding their types of malware that they put on the computer. In fact, it's so good that in the past, we've been notified by law enforcement saying, "You know, we thing something's funny going on with this computer," and we go and look at it and go, "Nope. Nothing's there." We scanned it with multiple anti-virus software, multiple anti-spyware software – nothing. And then put the machine back on the network, FBI calls again, "Um, it's doing that funny thing again," you know, so we couldn't find it. Ultimately, we had to just wipe the entire system but what they shared with us was that there was documents being taken off of the machine. We call this exfiltration. We didn't know exactly where it was going but knew it was going somewhere. So think of all those spreadsheets that you have on your computer that may contain sensitive information or e-mails that you have that may contain sensitive information. All these types of things may be leaving computers without our knowledge.

I have this habit – I wanna like, click the slide but you don't have slides. Okay. So now basically, a data breach is when sensitive information is disclosed either intentionally or unintentionally. And with that, you need to know specifically what constitutes a data breach in your state because every state law is slightly different. Now for the University of Hawaii, our definition is that

the information that needs to be disclosed is full name or first initial and last name in combination with either full Social Security number or your state ID or driver's license number or any type of financial accounts and in combination. So very, very narrow definition. We're not talking broadly, FERPA. We're not talking broadly, HIPAA. But with that in mind, if you have information of that combination that is accidentally disclosed or intentionally disclose or somebody hacked in and that information may have been available to them, as you may have a brief turn your hand which will require a notification to the affected individuals.

So but how many of you are here in the information technology sector, again, can you raise your hand? Good. For the rest of you, these are the people you look to for guidance to help you determine if a breach occurred because just because you find that there was information on a server that a hacker attempted to get into – they may not have been successful and your IT professionals will be able to help you assess that because trust me, if you have a repository of data, let's say 1.2 million Social Security numbers on a server and somebody attempts to break into it, you need to know if that data was accessed, right? Because in cases it may not have been touched at all, therefore you do not need to do a breach notification. Okay, so be careful. Do not declare every single intrusion or every single attack as an incident immediately.

Okay. So once you have determined that there actually is an incident, a breach, because – oh okay. Should I take this and walk? Oh, okay. Hello, testing, testing does this work? Okay. Oh, good, so now I can interview the audience. No.

[Laughter]

Okay, so basically, we're at the point where now somebody has declared that yes, there is a breach. So what do you do next? So what you need to do is notify your senior administrators as soon as possible, because you know who's gonna get the calls? Your university presidents, your senior administrators, your general counsel, as well as your Board of Regents. So all of those people in the senior officers need to be aware of it but additionally, you also need to begin the remediation process and in general, there is a whole series of steps and if I had the slides, I'd give you the links to where you can get some handy-dandy checklists and references but as Michelle Norin had indicated at the beginning, I also belong to Educause, the Higher Education Information Security Council – say that fast ten times. Okay and through that organization, they are creating checklists for things like an incident response

checklist, a data notification checklist, as well as what they call the information security guide and these references actually have specific case studies from other universities – Hawaii's not one of 'em, yet, until I can talk – but then, so these are places that you can go 'cause other institutions have already gone through this pain and suffering.

So again, first thing you wanna do is to mitigate the threat by removing the system, generally, from the network – and we don't say turn it off. We say unplug it from the network. Sometimes you may wanna bring in four and six experts who can then further investigate the system and they need the machine to be on because there's things in memory. Now, if you turn off the computer, they'll lose that bit of information. There is some very specific malware that lives only in memory and will be launched every time you reboot the system, so it may not be resident on your hard disk that's easy for you to find but it may be only resident in memory. So there's a lot of different technical things that you may need to have available for additional information to help determine if there's a breach or not a breach.

Okay, so again, some of the other things you want to do is to document the details of what happened. So when was it first discovered and how long do you suspect whatever it was started? For example, if it was malware on the system that then allowed access to a server that had the sensitive information on it, is a compromise desktop computer that was then used to hop on to the server on where your sensitive information lived. Well when did that desktop computer first get infected? So right, you wanna document this because if you do need to do a breach notification you do need to provide some details as to what occurred in your notice that goes out to your affected individuals, okay?

After that, make sure that you have a response plan, meaning that when you send out your notices, okay one the notices – the contents of the notice will probably be dictated rather breach notification laws in your state.so again, you need to know the laws in your state. So for Hawaii, it's very specific. We need to tell them exactly what happened, how many people were affected as well as provide them with guidance as to what types of actions each individual can take to protect themselves. So little generally be a list of things like, "Notify all of the credit monitoring bureaus so that they will be able to put on a fraud alert on your accounts and then also do a credit report on yourselves," right, so all this type of information is available in many different places. In fact, the US Department of Education has it available on their website

what happens if there is a breach. Also the Federal Trade Commission has that information, as well as the Educause resources. So people have put together these collections of information for you. And again, what you can do is e-mail me – write this down: Jodi – J-O-D-I at Hawaii dot edu. Okay, that's my e-mail address. Okay. Okay? Back that, everybody? J-O-D-I, J-O-D-I at Hawaii dot edu. Okay? And then I can also mail you the slides.

Ah ha. They got it. Okay.

Michelle Norin: So now that you're done.

Jodi-Ann Ito: So now that I'm – not quite done. Not quite done. But I and then winging it.

That, we can start there. Yeah. We'll just start there. Yeah, you can just go there.

Thank you very much to the technical team. You guys are great. Okay, so again, Hawaii – this is our requirements. Talked about that and we also, in the Hawaii notification requirements is if we are unable to notify every single individual, we do need to do a public, either press release or a website. So because a lot of times, students may have moved on. You may not have their current addresses; you probably do need to do this.

Okay, and so again, these are the things that we need to provide as part of the notice for your affected individuals – what happened. You need to provide them a place to contact in case they have questions and believe me, they will have questions. Lots of them. And this last bullet item about offering credit monitoring to affected individuals. That's going to be your institution's decision, okay? And many institutions have gone down that path. Some have not. So it really is dependent – because it is – that's a large part of the cost in terms of a breach. Okay and they could go up into the millions of dollars, depending on how many people were affected.

So again, remediation is you wanna correct the problem. So make sure that again, the computer is unplugged. You bring in your IT people to assess the situation, 'cause maybe it's not a breach, okay, very important. Make sure your data is classified properly and that your data is handled properly. How many of you walk into offices and you see like a form on somebody's desk that may have Social

Security numbers on them? Okay, I mean, this all happens. We live in –

[Laughter]

We will not identify them. We live in a culture in higher education. We're very free with their information. We're very open and sharing. This is our culture and this is part of the culture we need to change. In Hawaii, I come from Hawaii, right, so everybody knows everybody. Everybody's friendly. Nobody locks your car doors. We now lock our car doors. We now lock our houses and we need to do that in our cyber environment also. We are not in a friendly environment. Too many people are after our information so we don't leave papers expose on desks anymore. So what you can do when you see that, go up to them going, "Hi, this is sensitive. You probably don't wanna leave this on your desk. Just a friendly reminder." Let them know. But if they do it like five times in a row, then something else probably needs to be done. But again, it's changing our culture and it begins with each one of us, okay?

Education – we talked about having a security program and make sure that education component is in there. How many of you have mandatory training for information security on your camp- yay. Congratulations. You guys are fantastic. For the rest of you – we all need to strive to that. You know, we are working on something similar where we want to have every single individual at the university go through a basic information security awareness course, but you know, we still need to go through our unions and everybody needs to approve that along the way.

So these are some of the resources that I talked about. So we talked about Educause in general as being a place for higher education professionals in IT to gather and share information. The Information Security Council specifically around security and privacy types of issues and the information security guides. So these are the links that I talked about and again, if you e-mail me directly, Jodi, J-O-D-I at Hawaii dot edu, I will mail you the slides.

And this is brand-new to Educause. It is an incident checklist and it's really very, very complete because again, with the guidelines for what you would do should something occur on your campus. So you don't need to scramble and reinvent the wheel all the time. So this is what you wanna have handy before something happens and it talks about things like identifying the incident, damage containment, and data exposure assessment. How much

information may have been exposed. It talks about eradication and recovery, a little bit about notification and all of the follow-up activities that need to go on. So – and the remediation process will be long and onerous process because most times it's a changing of your business operations and your practices and more importantly, it's changing of our culture. Again, we are not in Kansas anymore.

The data incident notification toolkit provides some guidelines around what happens when you do have to notify any affected individuals. So it talks about sample policies and procedures and also have a lots of other links to resources that have been put together by your higher education compadres.

The data classification toolkit. Now this is important and you say, "Well, who needs to classified data?" Right? You all know that a Social Security number is sensitive but there's a lot of other types of information that people may not be sure. Is any parts – what part of a medical record may or may not be? What part of the students' education record may or may not be? Your campus may have different definitions in terms of directory information as it relates to FERPA. So these are all the different things that you need to know as well as understand who owns what parts of data, right, so now we're getting in a little bit about data governance types of issues. And then once you start identifying the datas, who has access to that sensitive data and is accessed we moved in a timely manner when that individual no longer needs access to that information?

How many of you have processes in place that if somebody leaves your organization or even leisure unit and is no longer needs access to sensitive information, how many of you revoke that access immediately? Oh, you guys are great. For the rest of you, something to strive for. Okay, and then again, though we need to make sure that security is not going to be a barrier to getting our work done. Okay? So it does need to be something that we constantly think about, even as we walk around offices. If you see a screen that has Social Security numbers displayed, make sure you tell that person, "You know, if you are not at your station, that probably shouldn't be there." How many of you walk away from your computers when you still have it logged into your e-mail? Okay, for longer than ten minutes? Okay. Sorry? He's not gonna say.

Audience: I've walked away from it but I've locked it.

Jodi-Ann Ito: Okay, as long as you lock it. Okay. So when I was in college, we actually used to go up to people's computers who was unattended and they were logged into that e-mail and I don't know where they went but we'd send them e-mails back to themselves just to let them know they shouldn't be doing that. So there's a lot of things that we individuals can do when we see behaviors that may jeopardize our data.

While a lot of breaches do occur because of physical and the system engineering types of flaws, a lot of our breaches occur because of humans, because of us as people, because we come from a culture where we are free and open. And again we need to change that as we move forward. I don't know that went through really quickly. Anybody have questions for us? Comments, thoughts? Yes? Comment.

Good comment. Thank you very much. So the comment is that you see Social Security numbers and e-mails or that it is retained if you were a faculty member and have old student records from who knows when, that it's still there and available. Again, so that's that point where we have to go through our physical drawers, our desks, our records – what do we really need to keep? Maintain only that which is legally required. So to me, it's always, "Are you keeping it because it's a convenience or are you keeping it because it's legally required somewhere?" And that's the distinction that we need. I mean, we keep stuff just cause it's convenient. Our hard drives are huge and we can do it forever and ever and ever and ever.

How many of you actually know what's on your computers? Yes? Every bit? I thought I did. I ran a software that looks for Social Security numbers. I was astounded by what I found. Oh my, oh my. So needless to say, I spent many hours cleaning it off. But we are, as part of our security program, instituting a policy where people need to scan servers for sensitive information, as well as if they wanna take it, they can't take that same software and run it on their desktop computers. We've had instances where they found huge repositories of Social Security numbers that they did not know existed on the computer because it was there from the person who left it when they left. So it's not even their Social Security numbers. Okay, and these are the things that we need to find and clean up. So we are in and the eradication stage where we are mandating that people go through and look for this stuff. We don't know where it exists, so we would like every one of you to look for it.

Here?

Male: See if this works.

Jodi-Ann Ito: Talk loud. Okay. Okay, you wanna take that first, Michelle or –

Michelle Iverson: Sure. I think the big thing – can you hear me? Is this on? Okay. With cloud computing, I think it still comes down to asking your provider and asking for an SLA. Asking for what they're auditing. If they're gonna put up a webpage for you, ask for them to give you – run those tools on the _____ page. Ask them to give you the reports from the scans to make sure that your sites are vulnerable to cross-site scripting or SQL injection attacks if they've got your database. Ask for independent audits and weekly reports. So when you're – those can all be part of your SLA when you negotiate that initial service. If they balk, hold your ground. There are a lot of free tools out there and, you know, I'll have to think more, but there are probably government resources, maybe Educause, other nonprofit organizations that might be able to help you as well and I'll think about that, too, but I think asking the right questions when you do buy those services is key.

Jodi-Ann Ito: Right, and so to that, Educause does have some guidelines around cloud computing types of questions you want to start asking yourselves before you engage in cloud services. It is convenient. It's very, very cost-effective and so the other things you need to think about is do you have policies around what type of data you will put in that cloud, right? It, again, comes back to your institutional standpoint and perspective. There are technical tools out there. Generally, it's called data loss prevention. So if you do do the data loss prevention techniques, what that means is you'll be inserting an appliance in your network that will look for this type of sensitive information as it's transiting your network, as it's leaving your network. Very expensive though, but again, there are, you know, more types of technical tools out there that may be of assistance for you.

Audience: Getting back to the cloud, there's an organization called the Cloud Security Alliance –

Jodi-Ann Ito: Cloud – thank you.

Audience: - composed of about 22,000 international security experts – ton of free information about the cloud, including the legal side, not just the technical.

Jodi-Ann Ito: Good point, thank you.

Audience: What is the name of it again?

Audience: The Cloud Security Alliance.

Jodi-Ann Ito: Yeah. Yes.

Audience: How about addressing issues regarding folks who take files home and security policies around that and also the fact that we, unfortunately, tend to keep files with records in them –

Jodi-Ann Ito: Yes.

Audience: - is pretty much the cracks and leaks you're talking about technical or do we – how do you address those others and are there lists for those?

Jodi-Ann Ito: Good question. Thank you very much. We don't live solely in electronic world. So, for us, we are revisiting our records retention policies because again, people tend to keep them forever and you kind of need to revisit policies every now and again to ensure that we only keep that information which is required. So for example, if you're paying for your to wish and with the credit card, do you really need to keep that credit card number as part of the record? No, probably not. You just need to know that the student officially registered at the institution, right? So with that, you also need to look at the places you store this information. Is it in the secured facility? Is it in a secured controlled facility? Do you know who has access to that room? Do you have any kind of security monitoring devices on that room? Paper does walk away. They do disappear and it's possible that people may tailgate into a secured area, too, so what kinds of controls do you put around that. But again, it's your process and procedures making sure that you audit that from start to finish, including the paper.

Michelle Iverson: And so I think also in addition to that, you do have to look at what your security awareness training is. So IT people always have to annual security awareness training but we maybe not everybody does it for their student population or their workers that are not part of the IT staff. So you have to get the security awareness broader and then you have to have policy, clear policy on what they can and can't do because you know, you can't control every human being but you can fire them when they don't follow policy. And so that has to be risk and consequences for not following that policy.

And I will tell you electronically telework is a hard problem and so we're dealing with that. When looking at some bandemic solutions, virtual drivers where it's kind of a boot disk type of solution – that's one we're looking at in partnership with DoD. We are looking at other technologies that do browser security and then it goes back to what I talked about, network segmentation. So I don't want those people who are coming from home who may – who are using those computers to go to all sorts of different sites that I may not want them –

Jodi-Ann Ito: Who knows where they go?

Michelle Iverson: - yeah, who knows where they go? That they might pick up , you know, Internet critters that we don't want on our networks. And so by segmenting, I can put in a DMZ and I can proxy so that those systems never fully touch the inside of my network and I can monitor that because of also segmented and I'm saying, "Anybody coming externally that's not one of my machines, I can put extra controls, I can put extra monitoring on those systems," and so that's why network segmentation is so important.

Michelle Norin: So one other aspect keep in mind is when you electronify your paper copies, which is a great thing, everybody wants to get rid of the paper and make it all electronic, think about what you're scanning in and what are the contents of those documents. We just went through our recent situation where doing a good thing, we scanned in all of our notes from one of our public meetings for the past 40 years and then thought we cleaned everything out but we missed some stuff and it caused us to have a formal breach. Now, where we have to notify some folks. So, you know, you try to do the right thing and get away from paper but part of that includes making sure we all understand what we're automating.

Audience: How do you get your administration to buy in to this? As you know, we're just _____ _____

[Laughter]

Jodi-Ann Ito: Yeah, right.

Audience: Everything's fine but these are the kinds of things that – I mean, this is proactive.

Jodi-Ann Ito: Right.

Michelle Norin: Yeah.

Audience: This is almost _____ financial institutional bank _____.

Michelle Norin: Well that's what I think it's important to have folks like Jodi-Ann, where you have a security officer. So – for the smaller schools, it might be a little more difficult to have a full-fledged office and a program but I think it's important to have at least one person in your institutional organization whose focused, at least some of the time, on security. So you can pick about policies, you can think about best practices – most importantly you can think about awareness because it really does stem and touch everybody and sometimes it has to be top down. Sometimes you need your president to put out a message saying, "Okay, we're gonna ha- everybody's gotta go through awareness training," or every – you know, "We're gonna have to protect our assets." You just need that positional force sometimes to get the message across.

So part of the awareness is to make sure you have messages geared toward different parts of your audience. Your security officers are usually the ones that do that and have those programs – Educause has some awareness programs and things like that. So yeah, it's not just your financial aid office. I would expect you guys, as offices, to work with your institutional IT organizations and mostly your security office if you have a situation or you have questions.

Jodi-Ann Ito: I think Bridget Ann has –

Bridget Ann Hemdon: Yeah, my name is Bridget Ann Hemdon. I'm the Deputy CIO at FSA and we knew that you all in the room would be the financial aid administrators but we felt as the panel has said, that everybody has a responsibility for security. We, from the administration side of the house, though, will be working with your presidents so it's going to be a top-down effort. We're going to embark in some form or fashion in doing security reviews of the various universities and colleges and that will happen probably beginning towards the latter half of fiscal year '12. We have started that effort with some of the guarantee agencies and we will continue to do that. So what we are trying to do now is arm you with tools and that's why these sessions are so full of links that you can go to because we know that at some point, we're gonna come in and we're gonna tell you, "You're not doing this, this, this, and this." But hopefully you're getting the answers to the quizzes that we will be asking in the next couple of months. So we understand that it has to be both bottom-up and top-down.

Audience: Is there anywhere that I can go 'cause you have like a – I'm pretty sure you gonna come in tell me what I'm not doing right but do you have like an audit checklist to tell me how I can check it before you come in and _____?

Bridget Ann Hemdon: Oh, of course. Of course.

Audience: Where would I find that? 'Cause I want that.

[Laughter]

Jodi-Ann Ito: Do your homework before they get there. Good idea.

Bridget Ann Hemdon: We all want that.

Jodi-Ann Ito: We all want that.

Bridget Ann Hemdon: Educause. And I'll –

Jodi-Ann Ito: So actually the other thing I would suggest is how many of you have internal audit units on campus? Work with them and ask them to come in and help assess you ahead of time. We're just starting that with the university. We've identified what we call high risk areas, which is one place is student financial aid offices and then we are working through our policy, our state laws, to make sure that they're going to be asking the questions along those lines. So that's something fairly brand-new for us. We have no idea how to be.

Audience: Hi, I'm Rodney Peterson from Educause. It's been referenced several times but the easy URL if you go to Educause dot edu slash security gets you to a lot of these resources but to answer the question, there is a self-assessment tool for information security governance that takes you through a series of questions. Not "yes/no," but, "haven't started, completed, in progress," to kinda give you and your senior administration a sense of where you are and what you need to do to get to probably a similar level to what the department and other external providers are gonna expect.

Michelle Norin: But again, I would encourage you all to work with your security offices and your internal audit offices. That's a really good point. Sometimes both perspectives will create a more well-rounded, whole-er picture.

Jodi-Ann Ito: Question here?

Audience: Question about the Social Security number. We know not to use that.

Jodi-Ann Ito: Right.

Audience: I have a staffer that wants to rely on the last four digits of the soch number. Does anyone have a position in that regard? We've not been able to find one. She's saying no, don't use –

Jodi-Ann Ito: Well, because you can reverse – if you're from very small states like Hawaii, you can reverse engineer the complete Social Security number from the last four. There are studies that were widely publicized. So while not a legal requirement, yet, if you can at all get away from it, don't do it. I mean you all should have institutional ID numbers, right? Separate from Social Security numbers, right? We are trying to convince every single unit in our university system to use those everywhere they possibly can.

Michelle Iverson: And you can let your CIO know that sooner or later the government will tell you you can't.

[Laughter]

Jodi-Ann Ito: State agencies. Interesting. We actually keep Social Security numbers because of our state agency. They process our payroll. So – we are working with them, too, but I don't know of a separate, federal legislation that would mandate states not use Social Security numbers. We still need them for taxes. We still need them to get paid. We still need them in a lot of places. It's how well are we protecting what we do need and only using it where it's required? And I think that's the thing. Social Security numbers have been sort of like our universal ID numbers across our entire country and that's where we need to get away from that. So, good question, though.

Audience: Jodi, how did you get buy-in from faculty?

Jodi-Ann Ito: Where are you? Oh, thank you. How did we get buy-in from faculty? It's a slow process. It really is a slow process. So I would engage them where you can. Meaning leverage incidents or get to the faculty senates or the faculty organizations. Leverage stories that you find on campus because they really don't want it to be them, either.

Michelle Norin: So we are actually – we went through a few use by example, awareness by example exercises and we've actually – my security

officers put together kind of a one-page, quick checklist kind of a document to issue to faculty to help them basically look at their machines and figure out and find some of that older data that might have sensitive data in it. You know, we've got faculty who keep class lists from 30 years ago or whatever and they forget. They don't know they have it. Something happens with their machine and so part of that checklist is to help them know where to look, what kinds of files to look at, to see is there sensitive data in the files and then basically rely on them to clean it up or work with the security office to figure out how to get the data off of their machines or protect it in a different way if it's research data or things like that. So we've taken a very targeted approach to the faculty specifically working through faculty leadership to target some messaging around that. And pointing to these examples where we've had issues.

Jodi-Ann Ito: So there was an instance where a faculty member unfortunately passed away and so staff was going through and cleaning out his office and then – how many of you remember IBM punch cards?

[Laughter]

Okay, so our course lists used to be on these punch cards. So this person was using those punch cards with Social Security numbers as bookmarkers.

[Laughter]

So once they found that, they had to go through every single book and shake it out and then shred the cards but, you know, it's again, that at least the staff was aware that this was an issue and then took the appropriate steps. So this is where all of us play an issue in recognizing what could be a potential situation and averting it before it happens. So anybody else have any other questions, comments, thoughts?

Bridget Ann Hemdon: Well I'd certainly like to ask that you give the panel a round of applause. Thank you so much.

[Applause]

There a few other sessions throughout the week that will give you some more information on this very hot topic so I encourage you to find some time to do it. Than-