Richard Gordon: My name is Richard Gordon. I'm the Chief Information Officer for Federal Student Aid at the Department of Education. I thank you all so very much for coming out today. This session is something that is very important to me and my stuff because what we're finding is that the management of privacy date, the management of data, we're not doing so well in the community at large.

So many folks are focused on well, we have to just manage the PI or we just have to manage that Social Security Number, when the reality is we have to manage so much more. If you look at what the federal government did under the HIPAA guidelines, which was a total sucker's space, that's in the healthcare space. They went down to the point of saying even conversations that you have on the elevator have to be managed, telephone calls have to be managed, all of it because any of that can translate into a leak, can translate into a breach, translate into a very problematic situation. And the education space, the number one – actually, in the number one place where your data is at risk is in education. The number one place where your data is at risk is in education.

Many of you who are Financial Aid Administrators that are working with data, you may print out a report that's got the entire loan profile for someone. I got to get out of the way of this thing. Loan profile for someone, you will set it on a desk, you will go out to lunch. That is privacy data that's sitting out there. What many of you may not know is that hacking of computers is at such a fever pitch that as you're typing in your user ID and password, your information is being captured and it's being reused. So you as a Financial Aid Administrator may have someone using your persona on the other side of the United States or around the world logging on as you, picking up access to millions upon millions of identity records, which is a huge issue.

This is not something that is being made up. This is something that is real. Every week in my organization we get notices from the US-CERT that says here's the user ID, here's the password that's used and here's where this account went in your systems. At Federal Student Aid, we manage 80 million loan records, 80 million. One of every five citizens of the United States, we've got information on. We've got information on you, all of you. So just think about it. If your identity is hacked into one of our systems, then your data is at risk. That IRS filing that you had, we've got that on file, it's at risk.

All of the information about your children is at risk. This is not something that we can ignore anymore. We have got to change the way that approach this. These kind folks that are behind me are going to give you some of the mentions of why this is important.

We're going to start with IRS, big *[Inaudible Comment]*.

By the time it occurs, it's too late. It is out of control. It's kind of like the WikiLeaks situation right now where Hillary Clinton is scrambling because of all those cables that were released, it's too late. Congress is saying, "Didn't somebody know?" I mean, this kid offloaded millions upon millions of cables, didn't somebody watch?" No, this did not and now we have to go into damage control mode. Dick is going to talk to you about that. Dr. Danny Harris is going to talk to you because as a CIA for the Department of Education, my partner in crime is going to say here's how you can protect – strategies that you can employ. You need to listen to these.

When you get to Cathy, Cathy Hubbs is the CISO for the American University, my alma mater, never told her that. That's where I got my graduate crease, see? See that smile? That's cool. She's one of you, she is from your side of the water. She's going to talk to you about why your CIO and your CISO at your organization are trying so desperately to put in protections, that they're beating up on you saying, "Listen, you can't share your ID and password. Listen, you can't share these paper reports." This is a big deal, but you're still not going to believe. I've been doing this for a long time, you're still not going to believe.

So my last partner in crime is Ira Hobbs. Ira's an interesting character. Ira what's the – so let me take it right from Ira Winkler. I'm sorry, Ira Hobbs is someone – okay, that's why. Ira Winkler is the President of Internet Security Advisors Group. He is considered one of the world's foremost – world's most influential security professionals and has been named a modern day James Bond by the media. Ira earned his reputation by performing espionage simulations where he physically and technically hacked into some of the largest companies in the world by investigating crimes – by conducting – investigating crimes against them.

Ira has written a book, has written books, is a Computerworld columnist and frequently appears on television. Brace yourself, that's what Pandora told me. So we had a conversation with the guarantee agencies, we brought in all the CEOs, CFOs, CIOs, Chief Information Security Officers and as Ira spoke, you saw

them kind of grab the edge of the chair like oh my, no it can't be that simple. It is that simple. When Ira unfolds this story, you're going to realize that everything matters. Every piece of paper, every phone call, everything where you say you just happened to bump into someone, it matters.

Ira's a no joke guy. This is an important session. Hopefully at the end of this session you will walk out of here and say, "You know, I need to go back home and take a look at what we've been doing." We need to shore this up. From the Department of Education side and year 2011 and going forward, we're gonna be talking with you a lot more about managing security, managing this privacy data. We have a responsibility to our citizens, to our millions upon millions of citizens to do it well.

You are one of those citizens. If it is not done well, it will probably be your data that is posted up. One of the things that you probably haven't thought about with the WikiLeaks stuff is that this kid offloaded millions upon millions of cables, sent it over to WikiLeaks, it's now all posted up. If one of your privileged accounts is leaked, just think about millions upon millions of loans records that end up on a WikiLeaks. That's your stuff, your name, address, phone number, the name of your dog when you were five years old, all of those questions that we answer. That's what's at risk so I ask you to stay tuned, it's going to be interesting. Take note, ask questions when we get to the Q&A side.

These people are very real. This is a very real issue and we need to do a better job so we're gonna open up. Actually I think we're gonna start with Dick. And we're gonna go to Danny and we're going to Cathy and then we're going to finish up with Ira.

Dick: Thank you very much, we appreciate being here. I tried to go out in the audience to make as many friends as I possibly could given the situation. And it's a situation frankly that anyone in this room could be in. We prided ourselves as a Federal Family Educational Loan Program Guarantee Agency, something that is not very popular at this point, but very important to President Obama's strategy because you can't forget all those borrowers that in essence still have Federal Family Educational Loan Program Loans.

And so we're part of the solution, not part of the problem. We thought that we had a very, very good culture of security and we thought we had an understanding in our company. Our IT, we

thought we thought was industry leading IT in terms of the security attached to that IT, but here's what happened for us.

How do you turn this forward? Right there? Okay. Oh, we're very behind here. Here we go. What happened to us is that we didn't have a breach in our facility, we have a facility that we rent from Imation in Oakdale, Minnesota. It's probably 106,000 square feet right now. We have guards that are 7 by 24. The facility had, at this point in time, cameras. The guards moved around, we had two safes in a locked room and over the weekend those two safes, which were 200 pounds each were removed. They included DVDs that included our complete database of borrowers, 3.3 millions borrowers.

That's the bad news, they were taken. The good news is they were recovered within 36 hours. The bad news is we didn't find out about it until a month later so all the things we're gonna talk about here are things that one should do in a situation where you have it, if you're, in essence, if you have this situation happen to you, you must react in a very structured way. The better piece is to listen to those of us who have had it and to ask questions. What are you doing differently? How are you changing the culture of your company? And we're gonna talk about those.

The cost, frankly, is significant. Had this data not been found, had it not been compromised and the law enforcement agencies do not believe that it was compromised, we would have probably had, without lawsuits, without Attorney's Generals coming after us and they did, we would have probably had well in excess of $30 to $40 million dollars of liability. It's very, very expensive for those PII.

They impacted significant – we put a call center in place, the impact was extraordinary from the borrower base because they were very, very concerned, our customers from our schools, from our partners, from the Department of Education, from the OIG and we'll talk a little bit more about those kinds of things. What did we do? Well, if this happens to you, contact a law enforcement agency, your local enforcement law enforcement agency as rapidly as you possibly can.

You should have an incident response planned, if you don't have one, you are in very serious disadvantage at this point so you should have an incident response planned. It should be managed at the highest possible level. In our company, our Project Manager, Executive Vice-President Project Management, she happens to be sitting right here, managed the process for us, Heidi Johnson.

And so it was controlled every single minute and be prepared for 7 by 24. Do not think you're going home, you are not. You are setting up a war zone and a series of war rooms and you are controlling as much as you possibly can while you try and mitigate any damage to your customer, while, by the way, you are still running a company. You can't forget about that piece.

We've retained experts in data theft and that's a very, very, very important to go to the outside, try and retain experts. We retain people like Morrison Foerster, a legal firm out of Washington, D.C. with offices in California so they're a national firm because the laws are incredibly complex on how you notify your borrowers, most of these laws, state consumers, what you do with the Attorney Generals and other state agencies. We did not know we had a national portfolio, for example, if something happens in the state of New Jersey, you must notify the state patrol, highway patrol. So there are all kinds of arcane pieces of – like registration data and you need help.

Also, you should have a crisis communication media manager because you have absolutely no idea how the press will descend up on you and they will. We retain Weber Shandwick and it was – this is a leading public relations firm. It's worldwide, we were very lucky to have the office of the headquarters in the United States in Minneapolis, St, Paul. Our headquarters, Oakdale, is in St. Paul. And we were able to set up with those individuals a basically 24 by 7 communications plan.

You should definitely consider retaining experts in physical security. And we did, we retained Pinkerton Government Services who came in and gave us a complete assessment of our physical locations and we have done that now with all of our locations across the United States and even though this took place in one location. On data security, we had FishNet Security and they came in and looked at our security and gave us recommendations.

One thing that I have left out here is that in our industry we have a regulator. You must, as soon as you are allowed, because the legal group that you start – once you start your law enforcement inquiry, they may tell you you may not talk to your regulator in which case that's what they told us. We had to wait until we were allowed to notify the Department of Education, which happened rather rapidly, but still I was very surprised that I kind of had a clamp on my ability to talk to my regulator, but you must – our regulator, by the way, it was not a pleasant call.

Our regulator found out, frankly, because one of the investigative agencies – it became a consortium – happened to be the Office of Inspector General, the Enforcement Division, very capable folks, they did show up at our facility and they are full-fledged marshals, they carry weapons. They are basically professionals in investigation so for those of us who run offices that don't see weapons in their offices very much, this was kind of an interesting change.

You definitely want to establish guiding principles and you want to establish those guiding principles frankly before you have a crisis of this type or any other type, but especially security crisis. The first principle is that the CEO, in this case was me, has to take absolute full responsibility and be the leader in charge of any response. That means that generally the CEOs in front of the television cameras, the CEOs answering questions, the New York Times, the Wall Street Journal, Chronicle of Higher Education, and a score of other high quality news media inquiries.

You have to be transparent with not only the Department of Education, but you have to be transparent with all of your industry partners so we'll talk a bit about what we did there. You have to ensure the highest possible support for your customer, for your borrower because that is the essence of the failure here, to protect borrower information, Mr. Gordon was talking about. You have to cooperate fully with law enforcement agencies. We executed our incident response plan. We executed our communications plan, which we had all ready to go for a crisis. We worked side by side with the Department.

By the way, I've never seen so many Department of Education personnel in my life and I have been in this industry 37 years. I met people, I said, "I don't know. They're legion. They are legion." They just came out. Not a single person that came from the Department of Education, and Wynonna was in charge of it, very, very, very interesting leader, but not a single person came to do anything but to help us get through this crisis. It was – without the Department of Education, it would have been difficult for us to do what we did.

So not that I'm suggesting you do it to get noticed by the Department, please don't, but it was good to get noticed. Folks, like these two gentlemen here, folks – I see Diana's in the audience, I see you're in the audience. There's lots of people in the audience, but Charlie Rose – anybody know Charlie Rose? I didn't know who Charlie Rose was, well he's a general counsel for

the Department of Education, so you get to meet a lot of different people. The corporate communications people, Mr. Taggert, Mr. Ronse, you'll meet everybody and it was just a very good process overall.

With that then, we have some recommendations that we'd like to give you and those recommendations are – it could happen to you. If you don't think it can happen to you, shame on you because it will. I think you'll hear that in a few minutes. This happened to us on 3/21, the weekend of March 20th, March 21st.

And since then, we have taken extraordinary pains to review all of our policies, to train, to change our culture, to change our physical layout, to change our systems layout, to be just as protective of our data as we possibly can. Not just PII, all data. There are no machines in our company that aren't encrypted. There are no PDAs that aren't encrypted. We have a whispernet, cybernet kind of arrangement so we have a – our WiFi is not in any way connected to our system. We have multiple, not one, but multiple ways to logon to a system, including tokens and badges and all kinds of interesting things. We have put remote monitoring in for any movement of PII data of any kind. We have done data leakage software and installed that. We have done data masking so that if you don't need to know all of the data when you do work, whether you're in claims or you're processing a default diversion request or whatever it might be, it's masked. We do PGP encryption to everything that possibly walks and yet I have walked in my facility and done exactly what Mr. Gordon's said, exactly.

I have found PII on the desk when someone went to the bathroom and what do I do with it? Cause I'm the CEO and I'm a friendly person. Some folks probably know that as I've walked around. I pick it up and I take it back to my office and then I call and I say, "Now I was in this unit, who's the supervisor for this particular person? I'd like to see them. Who is the manager?" And once generally I get to the manager I know who they are. I say, "Bring these people and bring this officer in, I want to talk to them." And that's the only way that it will happen. I challenge people, I open a door in my facilities and I open – and I have ten people behind me and I say, "Come on in." I'm asking them as a CEO to come on in and they don't because you must badge in and you must badge out.

And so you have to change the culture by walking the talk. I heard this young man's presentation at that same conference, Mr. Gordon talked about and it was a wonderful presentation and he kept using the phrase that I would change it a little bit, but he'll give it to you

today, but this person, "It's stupidity that gets people." And I would change it to this, "It's not stupidity for me as much as it is you're just not thinking about it every day." How would you like your personal identifiable information lost? You wouldn't and so do everything that you possibly can to make sure that that doesn't happen.

We have security officers like I'm sure you do, risk people, like I'm sure that many of you do. I was talking to Penn State, they had a PII incident. This is very interesting in the sense that we have caught the – we didn't, the law enforcement folks have caught the individual who was involved. That individual is pleading guilty. He has tapped his two co-conspirators in this. We'll find out on the 13th of December whether there's anybody inside. The law enforcement agencies have said this, "That no ECMC current or former employee has been involved, but we will find out how this happened and why it happened." And you know, it could well be, and I'm just at this point saying, could you ever think about this? If you have a vendor coming in and the vendor's moving wire, cause we all do that right? We move wire through the ceiling, you have a vendor coming in because one of the bathrooms is stopped up and you need to get a plumber in. You have a vendor coming in for 400 or 500 activities in a year. That vendor sees something that attracts him and says something in a bar and that's all it takes.

I'm not saying that the vendor is not – so now vendors come into our facility, everybody has to be badged. Some of our badges we know exactly where the vendor is and no vendor is unescourted in our building. And so that changes our culture dramatically. Having the inability to go on the internet when you're on the system changes your culture dramatically. It also causes reduced productivity and so you're looking at ways to deal with that issue and so this is the 21st century crime.

We, in essence, you either – remember Psych 101, recency, primacy, you know, either to be the first or be the last. We were the first. We aren't going to be the last. Thank you very much.

Danny Harris: Good morning everyone. Let me start by thanking Richard and his FSA colleagues for inviting me to Florida because I hear it's freezing back in Washington right now. And I'm actually trying to work out a telework program with my bosses Arne Duncan and Tony Miller for me to stay down here in Florida and jus telework back to Washington. As you could imagine that's not really – the negotiation isn't really going that well.

So let me do something a little different there if you don't mind. What I'd like to do is I'd like to start at the end of my presentation and go back to the beginning. And I think you'll understand why after I get through it.

So here is the moral of the story. If you and your organization are combating cyber crime with only technology, you will lose the battle. Let me do it one more time. If you and your organization are combating cyber crime with only technology, regardless of how good your technology is, you will lose the battle.

And so let me borrow a very trite expression from my friend Yogi Bear and Yogi says, "At the end of the day, only people can prevent cyber crime." And so let me tie those together with PII; 500 million sensitive records breached since 2005, 130 million credit cards stolen from Heartland Payment Systems in January 2009, 130,000 student records exposed, 32,000 ed customer computers have been victims of keyloggers and Richard talked about that a little earlier. In other words, when you get on and start keying, all of that information is being picked up. 32,000 since 2006 and more and more every day and those are the ones that we know about, by the way.

Those are the ones we know about. A noticeable increase of cyber crime activity targeting government compromise of PII. There was a time at the Department of Education, and I've been here for 26 years, there was a time where criminals weren't really interested in us. And then all of a sudden they became very interested in us. And why is that? The same reason why bank robbers rob banks. It's where the money is and so all of a sudden we've become very, very, very serious about cyber crime.

Top ten cyber crime complaints, non-delivery, auction fraud, computer fraud, check fraud, Nigerian letter fraud, the average monetary loss per fraud complaints, it goes to the millions. So what is PII? And this is still debated today and a lot of folks are really confused about what PII is.

Here's kind of a snippet of what we would consider PII. Full name, street address, vehicle registration number, biometics, digital identity, Social Security Number, but we have to be very careful about defining what PII is because when you put a certain number of attributes together, in aggregate they become PII so don't assume because your SSN number is not part of an aggregated bunch that you're not putting PII out on the street.

From Computerworld August 12th, "Human error causes roughly 70 percent of the problems that plague data centers today." 70 percent whether it's due to neglect, insufficient training, end user interference, tight purse strings or simple mistakes, human error is unavoidable. The management of operations is your greatest vulnerability, but also is a significant opportunity to avoid downtime. And the sentence is probably the most important. "The good news is people can be retrained. People can be retrained."

So what have we done at the Department of Education? The most powerful thing we've done is working together from the CIO perspective, we've worked with leadership to change the culture and change the perspective about who owns the battle against crime. Who owns the battle against cyber crime?

There was a time when the battle belonged to Richard and I. We don't own the battle. Information assurance, IT security, combating violations of PII is every employee's responsibility. And so how do you build an awareness program? That's where it all starts. Again, if you have incredible technology, but the individuals who manage that PII aren't trained, then the technology won't do you much good.

So how do you build a strong awareness program? You establish program goals, you develop information assurance topics, you develop delivery methods and you establish program management. I want to walk through each of these fairly quickly. So first of all, establishing program goals, communicate and clarify the organization's overall intent to secure its information resources, provide information about security risk and controls, promote staff awareness of their responsibilities in relation to information and security.

How many of you in your organization require that every single employee take a course every year on information assurance and IT security? Let me see a show of hands. Okay, that is simply not enough. I see about 20 percent of the hands going up. That is simply not enough so I'll get to some recommendations, but I'll make one strong recommendation to you now.

The first thing you should do when you get back to your organization is talk to your CIO organization or Officer of Management, whoever manages your IT infrastructure and ask them to show you what your awareness program looks like. You should have a manual that says, "Here is what our awareness program looks like." And if those individuals tell you that you

don't have an awareness program or if they scratch their head, you should immediately go to the highest person, the highest ranking person in your university organization and ask to develop an awareness program. Motivate staff to comply with the organization security policy and procedures.

Let me tell you how strongly we take that. Not only must everyone take that class, we get a feed about two weeks before everyone is due to take it and that information goes to the secretary. You do not want your name on that list of individuals who did not take your security awareness class. That's how serious we are about it.

Second develop information assurance topics, policies, make sure everyone knows about the relevant laws, background information on fundamental information security concepts, news of significant security events, advice on maintaining home computer security. That's one of the hidden items. That's one that folks typically miss, but keep in mind, how many of your folks go home and continue to work? How many of your folks go home and log into your institution? They're simply bringing in criminals with them if you haven't trained them properly.

Emerging information security risk and provide case studies so people understand that this is real, it's not made up. It's real. Third, develop delivery methods. Just the class is not going to do it, just sending information is not going to do it. Provide monthly e-mails. You have to continue to bombard folks so they understand how real this is. Internet delivery, newsletters, screen savers, brown bag workshops, security expert panel discussions, branding and new employee orientation. How powerful is that?

The first day on the job, those individuals get a presentation on their responsibility of combating cyber crime and specifically protecting PII. And establish a program management; every institution should head a unit who's only responsibility is to manage cyber security, protecting PII and everything that falls under Information Assurance. If your organization doesn't have one, you need to talk about developing one.

Develop tools and techniques to fill the gaps, implement across organizations. Measure improvements through assessment tools, very, very important. Maintain and update tools as program needs change and so let me run through some best practices that we've used and the thing that you really have to understand is none of this is new. You don't have to do this by yourself. You don't have

to reinvent the wheel. Putting a program together, there's tons of information. And if you can't find it, you can reach out to Richard and I and we will help you put a program together. We will provide you artifacts that will allow you to easily put a program together.

So best practices. Protect each customer's PII from inappropriate exposure or sharing, senior management ensures that staff understands its serious about protecting customer PII. Folks, it has to start there. Again, if you provide this responsibility to your CIO or to your Office of Management Executive to drive, it is not going to work. Your probos, your CEO, your COO, those are the individuals who have to drive this as an organizational priority.

Transparency, inform customers about PII use and protection. Give customers information about the Department, what the Department is doing to protect your PII. Check and check again. Here's a powerful one. Only collect required PII, reduce duplicate requirements. As you develop new applications, new programs, as you modify new programs, the first question you should ask is for every data element that you plan to collect, not just for normalization sake, do we really need that piece of information?

The best way to protect PII is to not collect it at all if you don't need it. Again, the best way to protect PII is not to collect it at all if you don't need that data element. Establish computer matching agreements, interagency PII sharing will help you combat the proliferation and adhere to local and state legal requirements. And then finally from the practitioner, from the end users perspective, what should they be doing? What are the simple things that you can tell them and educate them on?

One, you've got to help them recognize what PII is because most folks don't know. Stop, think, and click. In other words, when you're using systems, stop and pay attention to what you're using, think about the information that's being asked for and only proceed if you're comfortable that there is no PII that you shouldn't be passing forward.

Individuals should know what a breach looks like and they should report that breach quickly. Ron talked how time was of the essence in terms of catching up with the criminals. Transmit PII securely, store securely, dispose media properly and finally adhere to strong authentication.

I will end with a repeat. Regardless of how strong and how powerful your technology capabilities are, if your folks aren't trained, all of them, not the technologist, all of them, then you will lose the battle. Thank you.

Cathy Hubbs: Good morning everyone. I also want to thank FSA for inviting me down. My name's Cathy Hubbs, I'm the Chief Information Security Officer at American University. So I hear – how many people in the audience are from universities?

Okay, so I didn't even really realize that. So it's been interesting listening. So far it's been a great set of information that's been provided thus far. I think I was invited down to kind of give you a perspective of one university is doing and hopefully it will give you some satisfaction that we're doing some things right. And I thought it was important since you all work in different universities, we're all in different shapes and sizes, but I think it's important to think about the complexity when we think about all these potential incidents and ways that cyber criminals are getting at us. We need to think about these environments and just how complex they are and what's required, it takes all of us, technology as Dr. Harris was saying and humans.

So at American University, we're in northwest D.C. and we have 11,000 students that are actually attending, give or take. But there's about 30,000 with alumni that could be on our systems with accounts. We have about 2,600 faculty and staff members. Some of those are adjuncts, as you can see we also have parents, alumni, visitors, visiting researchers, all those people are coming on our campus either physically or logging into our systems so think about all that.

We also, I think, heard about vendors coming on, not just physically but sometimes they need to come in and assist both the technologist and different departments with projects and applications that they're using, software applications so we've got all this kind of human interaction with our data sets potentially and on our network that we have to think about.

In addition to that, we think about all the different end points in a university environment, which is different than maybe a regular business. We have students that are coming in with the latest gadget right? That's network enabled and has their data on it, potentially plugging in or wirelessly connecting to our network.

And, of course, because we have different research going on, we have all the different operating systems imaginable at most university. So we're dealing with a lot and mobile laptops, desktops, et cetera. At American University, in addition to having our – actually we're a midsize university, but we have about 51 buildings on our various locations in northwest D.C. and we also have dual data centers so that's kind of where our data resides.

In addition to that, I'm sure you all are aware the complexity of a university is the different types of data sets. He was talking about – Dr. Harris and Mr. Boyle were talking about compliance. They were talking about health information, for example, but he's talking more broadly about personally identifiable information. Well, in a university, of course, and with this audience in particular, we're thinking about student data. But remember, we are a business, so we also have health information, we have athletics, we have the staff and faculty members have a benefit program so we have health information, we have financial information, we have student information, we process credit cards, so there's a plethora of laws and regulations out there and different types of personally identifiable information that we're responsible for protecting.

So in our environment, we realize that technology alone will not protect all this data so some of the approaches that I like to take is working with the various university stakeholders. So when I first started in 2007 at American University, we had an IT security team and that was made up of representatives from general counsel, we had them from the student Financial Aid Department, we had them from the Registrars Office, we have it from Public Safety so we have the police representations to the physical side, risk officers, a lot, all the various – there was about 14 of us and we come together quarterly to talk about the various risks or concerns about risk from those individual business units and then we talk about the different programs and plans that we're working on to be able to manage those risks.

So I find that to be incredibly important. We're moving that into an enterprise risk management team so that it won't be just focused on technology, but thinking about holistically about all the risks, the risk to the university moving forward. But part of that is also cyber security, digital data, protecting that PII and what are all the various departments doing and their responsibility so we think that that's very important to have regular meetings throughout the academic year and throughout the entire year to be bringing all these various stakeholders to the table to talk about what their

individual business risks are and what the university risks are and doing our plans and programs around that.

We also have an emergency planning group that meets every three weeks and this is for strategically thinking about business continuity, disaster recovery. We walk through and do tabletop exercises. When Mr. Harris was talking about incident response plans, I wrote a little note and I wanted to say to the audience it's important to make sure that your institution or your organization has an incident response, an emergency planning team, whatever you call it. But if you don't know who that is, you should call and find out, figure it out. Call around, determine who is in charge of that program so you may be the one that notices some sort of a breach or at least suspects a breach. You need to know who do you call and what's your individual responsibility and hope that there's an organization – not hope, but ensure that there's some group out there that's regularly doing this. So we meet every three weeks and we have different agendas.

I'm sure most of you heard about the shootings down at Virginia Tech a couple of years ago. That became front and center at our university. That was one of many things that our emergency planning group worked on so we're constantly moving the university forward and reflecting on the various plans and actions that we have from physical to cyber security incidents and everything in between, business continuity and disaster recovery. So we have that in place.

I can't remember if it was Dr. Harris or Mr. Boyle that was talking about the need to have somebody in charge of the cyber security program in your enterprise. Well, my position is in charge of the IT security program, but it goes beyond that. It bleeds into the physical world to be sure as you've heard from the first two speakers. So I work very closely with both our general counsel and our risk office managers. So we don't have formal meetings every week, but we call each other regularly. So if there's a new regulation or a new adjustment to something out in the law or we just hear something that's happening on campus, we have very strong ties to one another so that we can approach it from the law perspective, from the risk perspective, from the public safety and the physical security aspect and the technology. So I think it's very important if you don't have one risk officer identified in charge of a program that takes care of all those parts and pieces, make sure that you can identify who those individuals are that are responsible for those parts and pieces and make sure that they're talking and it's not siloed.

So the other thing that we do is I am in the Central Information Technology Department and so we as an organization reach out to the different departments that have IT support and we meet with them regularly. We have a listserv and we also meet every couple months to be able to bring up dialogue and talk about the different products and tools that we have available to share with one another and any concerns that they have so that we're – this is a continuous process.

Security is not a destination, it's a journey and you got to constantly be working it. It can't just be every few months that you touch on it, so these are some of the ways that we work on it regularly through these various communications and groups.

The other thing that I think is very, very important is in addition to the security awareness type plans that Dr. Harris was talking about, I think it's important to get down into the deep processes making standard repeatable clear transparent processes for all the workers, for all the offices that are processing and handling this PII. That, to me, that's the win. Security awareness, quizzes every couple months is super important. Security awareness training once a year is really great, tends to focus on passwords and things that are very important to us, but what are you doing everyday role based? And do you know it very well and are you understanding where you get to that piece where there's some sort of data that should be protected and do you have a repeatable process for handling it?

So one thing is the university didn't have in place was a repeatable process for even bringing new policies and procedures into place. So that that's a template. Anybody in the university can bring something to the table and say, "We think we have a gap here that's not documented. We have oral history about it, but we're not sure everybody knows." So we set up a process so that anybody could bring to the table a policy and a procedure, a guideline that made sense to the university and have that stored in a central location that everybody could have access to.

We're big, heavy in the central IT about least privilege, talked about masking data. It's also important to – if you don't need it, don't hold onto it. That's what least privilege is all about right? Making sure that on the technology side and partnering that with a process – if you don't have access to Social Security Numbers and a name and a date of birth for your work, then ensure that technologically that's not being delivered to you and from a

process standpoint, when you're actually doing account creations that that's not accessible to you.

So we have data custodians that are identified throughout the university that are responsible for different types of data sets and they're the ones that authorize access to those types of data sets and we track that. Does that make sense? So we actually have responsible identified people across our organization that they're the ones that authorize that access and then it gets processed and we make sure that that's conformed to. So we have a very well audited process.

In addition to that, change management, something that we're very heavy into, so everything that's made changed to our applications, our software, our hardware, our network environment, we record that. We have a Change Review Board that meets weekly so we're very detail oriented to make sure that there are insider threats as well, right? So it's also a service, customer service thing to make sure we have up time, but there's also an opportunity to look in and make sure that nobody's tampering with our services and our hardware so we do change management very regularly.

And then my favorite is the system's development life cycle. We're constantly bringing new services and new applications online to help our constituents and so we want to make sure that security is at the table from the moment a decision is to bring a new application online. We want security from the beginning to be thinking and asking the questions about what kind of data's going to be processed with this service? Is that going to touch our sensitive data sets in our data bases? And really start from the very beginning and walk through from the time we're either going to outsource to another company or whether we're gonna in source, how it may touch our systems and our sensitive data all the way through to the moment that we're gonna purchase it and then we're gonna bring it in and own it and manage it and what are those controls and adjustments that are gonna need to be place to the training of the individuals that are gonna be interacting with it.

So we're big on – and it's a maturity curve right? There's a lot of people at the table, but we say it over and over again, come in at the very beginning. Don't bolt us in at the last minute when we say, "Oh my gosh, you're about to go live next Wednesday?" "Stop. Social Security Numbers are flying in the clear. We can't do that."

So if you have security professionals that you work with, please, please, please invite them to the table at the very, very beginning of the process and throughout it. Then they won't have to be like police people putting their hands up going, "Stop. Not now." That's how we get a bad reputation of being the bump in the road and being in the way of you being able to get your business processes done.

If you bring us in at the very beginning, we can help work with you carefully to build a system that accomplishes your goals as the workers and your business objectives while at the same time protecting the sensitive assets.

We've really tried to have this transparency about service level agreements and that includes secure ongoing security assessments, office level agreements, memorandum agreements, everything, to really make sure that every single person at the table understands what their role in the responsibility is. We do contract reviews. Our purchasing office has brought security into the table, so we're reviewing the contracts as well to make sure that there's language in there that fully protects us.

Big on risk assessments whether they're internal, or external, there's a produced called Shared Assessments that's been used in the financial industry for a very, very long time that's well vetted that we're starting to use in higher ed and in particular American University is stepping out in front and that's really for – I'm sure you guys have heard about Cloud Computing right? More and more we're putting our services out to Cloud providers. Well, how are we assuring the security of that data? A lot of people are going, "Ooh, we'll just kind of transfer our risk by putting it out there." Right? Well, how do you protect that? How do you know? Where's their data center? Are they using encryption? Are they doing security awareness training for all of their staff? Et cetera, et cetera.

Shared assessments is a very unique interesting tool that's very holistic that goes around their physical and their various security measures that we've done on five different programs so far and we're attaching it to the contract so I'm happy about that. It's not perfect, nothing's 100 percent, but it's on our way.

And then general security awareness, a lot of the things that Dr. Harris was talking about, we do as well. And from technology, we use a network access control. I'm not sure how many of you are familiar with network access control. Not to get too technie on

you, but we have wheres I described our wireless and wired environment. We have a lot of people coming on and off our campus. We actually make everybody authenticate so everybody, to get access to our network, you have to log in. We have visitor accounts. Those visitor accounts, you have to have somebody that's a member of the university vouching for you, if you will, to be able to use our internet.

If you're a visitor, of course you don't get access to much except for the internet, but it's the way to track your name and contact information in case you do something nefarious because you are on our network and you have an IP, a computer address associated with the university so if you're doing something that's less desirable, we want to have a way to track it back to a time that you were there. So we do that.

When you connect to our network, you go through a very brief - what we call a health check – that does some very quick checks to make sure your running anti-virus, a local firewall and making sure that your browser and basic applications are current. And then we do hold this encryption and we're doing regular patch management to make sure that those third-party point products like Adobe and Flash and Java, these are probably familiar to you, I hope. You use them every day. They seem to be what the cyber criminals are loving most right now. Why? Because whether you're at home or at work, these are on everybody's computers and they're the last thing that people get those little annoying pop up boxes that say, "Ooh, you need to update Adobe, right?" I'll do that later. I'll do that later. Well the cyber criminals are totally down with that and they are just swooping in so we created in June a way to regularly patch our end points. We've got about 4,000 of our systems of American University owned systems and it was a big deal because open universities – universities are very open. People don't want us to touch their systems. We had to tell, "It's for your own protection." So that was a big win.

We close unused ports so people can't just walk around all – you can imagine at a university, all of you work there, how many buildings and rooms do you have with little jacks on the walls, are those actually all live? Can anybody plug in? In our case, people would have to authenticate, but that's something that a cyber criminal could easily just be connected. And then we log a lot of the activity on the various systems and then we have – one of the biggest things is everybody's moved to web application services.

And something that a lot of businesses have not quite done yet is continuous web application security monitoring. This is really the frontier right? We're trying to leverage the power of the internet in the worldwide web so what are we doing? We're transferring all our services up so that people can log in and do that there. But we're not doing the backend due diligence to make sure that cyber criminals aren't taking advantage of the weaknesses. So those are some of the processes and here's a few more firewalls and the usual stuff that we're doing.

So, as you can see, we've kind of got a balanced approach. We're working with both our end users with security awareness a lot like what Dr. Harris- I won't repeat that. We've got a lot of groups in place, established that are constantly looking at different perspectives of the potential risk that regularly communicate in the event something happens and hopefully preventatively and as you saw, several technologies in place as well. So now that I shared what AU does, I'll let Ira scare you.

Ira Winkler: Hi, how much time do I have? Okay, okay. Let's see where I begin. Sorry, got to wake up. Okay, so first, I was really pissed off when I saw the agenda. I mean, I looked through it and sorry, I'm from New York. This is how I talk, get over it. And you know, people from Texas, sorry. Anyway, basically I looked at the agenda and it said pretty much this session is for if you're an IT person which frankly is absurd, stupid and I couldn't – this is a session that everybody should be trying to encouraged to attend. Now only if you're an IT person if you look at what the agenda said. Cause, you know, you hear like – I'm bad with names - whoever the first guy was who spoke at the general session.

He said, "Protecting PII is one of the top things they're looking at," and then oh yeah, "Just be concerned about protecting PII if you happen to be in technology," which is the stupidest thing I've ever heard. Okay, let me talk – I mean, people basically go ahead and pay me to rob them blind. I was introduced as hacking. I don't really hack, hacking's boring, it's too easy. I generally go in and do black bag operations where I'll physically compromise the site and rob them blind and maybe I'll do some hacking along the way, but along the way I'm talking to people, manipulating them, getting them to point me to the right directions and all that sort of stuff.

Let me see if I should talk about stuff. Okay, so first people think the data they store is pretty much worthless and after awhile it just becomes too commonplace. Everybody starts thinking that, "Well,

I have this data. I have that data." And it's really easy to just ignore the data after awhile because you're looking at Social Security Numbers all day, you don't give it a second thought. And then some people – when I was originally gave this some form of this presentation, the first time, I was talking to I don't know, it was a bunch of contractors or vendors that FSA has as far as people who administer loans or something like that. And they didn't think that they really had to worry about a problem because nothing they protected was sensitive.

It's kind of like the absurdity of the nuclear agents, like the nuclear power companies. They went ahead and said, "You have to be compliant with these security regulations, but only if your systems are mission critical. And if you aren't compliant, we'll fine you a $1 million dollars a day." So what all these power companies did was they sent back a letter saying, "We have no mission critical systems so don't worry about us." True story. So anyway, self-regulation, that's what you get. So same thing with a lot of the vendors that FSA has, a lot of self-regulation going on there. Not a good thing.

Pretty much what you got to understand is the bad guys come after data in whatever form it's easiest to get the data in. Again, PII has lots of value. It's really easy to steal lots of money once you have some basic PII and all that sort of stuff. I'm guessing you know this thing. Anyway, the value of data is relative. People keep trying to second guess what's value to somebody. It's absurd to me, like when I'll talk to people, they think, "Oh well gee, nobody cares about this," or "Nobody cares about that." I'm like, "Great, that's how I'm gonna start to screw you over first. Just tell me what you think is not sensitive and that's what I'm going to come after first."

So anyway, I'll talk about this and you'd be surprised about how little inconsequential data adds up to major value because too many people think what happens is it's like oh well, this data's not that important and that data's not that important, but when you start thinking about it – cause my background is from the National Security Agency. And I started out as an intelligence analyst there and I was looking at little pieces of data and basically little pieces of inconsequential data, when put together, give you major, major intelligence value. It's not about getting the one big thing, it's a lot of little things going on here, there, and there and a whole bunch of other places.

Frankly, I took out case studies and I don't even recognize this presentation anymore, someone edited it. It's like the presentation was kind of phrased the way I talk a lot and that's not there anymore. So let me just – so basically let me describe it this way. So when I did the - let me talk you through a couple penetration tests.

There is one pen test I did where we were trying to compromise a company that made power systems. And so what happened was the first thing is they have a nice big welcoming lobby and so first thing was to get past the receptionist so I just like walk in with a friend, act like we're both talking on cell phones and walk right by the receptionist. So she's like, "Excuse me. Excuse me." And we just go in and follow people in through the morning rush hour. So then we find the big empty room, get on the phone, call up the operator and say, "Hi, I'm the CIO, we need two contractors to get badges. Where do we send them?"

They forward me someplace, I don't know where it was, turned out it was ironically the front desk and say – and then I'm like, "Hi, I'm the CIO. I have two contractors who need badges." She's like, "Okay, send them down. We'll have those –"so we go down – oh this, she's like, "Oh, I tried to stop you two." "Oh, I'm sorry. We were on the cell phone." She's like, "Oh, I thought so." So then we're starting there and there we are, and this guard comes over and the guard's like, "You two need badges?" It's like, "Yeah."

So we go in this room, get badges and then she takes our pictures. She's like, "What do you two do?" We go, "Computer stuff." She's like, "Oh, do you need access to the server room?" I go, "As a matter of fact, I do." So she goes ahead and like she gives us these badges and then she programs all this stuff in and then what happens is she's like, "Well, it'll take a couple of hours before all the accesses are enabled." We're like, "Okay, we'll wait." So anyway, we just go back up to our room, hang out like hack the network for awhile, then we try to find out where the server room is and we're just wandering around.

We find the server room; it's logged on with all these systems in the super user mode. We walk in there, add a user to the network and then super user, administrative privileges, then walk out and pretty much we hack the whole network. So anyway, once you have one super user on the right system, you have full control. So that was pretty much half a day to compromise a lot of not nuclear stuff, but a lot of power plants throughout the country. We knew

exactly how they were made, the designs, all that sort of stuff. So anyway, a couple of weeks later I get a call from this guy, who says he's in charge of security for the building and he's like, "Hi, you were here and you – somebody gave you – I want to know who gave you the badges." I go, "I don't know who the hell you are and I'm not going to tell you anything." I go, "Even if I know who the hell you are, I wouldn't tell you this. I would tell the CIO that because he's my client and so if you want to tell the CIO that you want to know who gave me the badge, go ahead and tell the CIO and we will tell the CIO who will tell you. And then on the other hand, when the CIO calls up, I will let the CIO know that not only was a problem that we got badges, that it's a bigger problem that you don't have any idea who gave us the badges in the first place." So anyway, I never got a call again so.

Then there was another test I just did like a couple weeks ago and this was a test and this involves a university ironically and I wasn't breaking into the university. I was breaking into this group that did statistical analyses and so we found their building. Well, it was like me by myself this time. They do statistical analyses and they want to find out what we could find out about them. So anyway, it just turns out, little side note to this whole story was, that they had a building and across this courtyard was another building that a university was in and the university had classes in that building and a whole bunch of other stuff.

So I decide to wander into that building, go up to like the floor that's pretty much directly across from my target, with a camera and just start taking pictures across there. There's a whole bunch of classrooms there, there's a bunch of offices, go late at night because obviously when you go late at night, you can see better into windows which have reflective materials.

So there we are and it's probably not even late at night. All the evening classes started to wander in, but I'm wandering around all these university offices. And there I am going through there, I could have put like these little devices that could have just pretty much tapped all the keystrokes going in and stuff like that. But the university just kept letting things in, or letting people in because, of course, people were going back and forth. Not everybody had offices, people had their open area like I don't know, what do you call those open area things? Kind of like a cubicle farm type of thing?

So there I was taking pictures and I'm like sitting there cause I really didn't like doing it because I wasn't there to compromise the

university, it just so happened to be very convenient. So but there I was pretty much able to hack into the university network at will and they weren't even my target. And ironically one of the reasons they wanted me to like do this statistical company was because they tend to do defense work and I wasn't supposed to theoretically know that. But there I am doing things, taking pictures of their blackboards through their windows from the university and then another thing that happened was then I kind of get in the thing cause ironically and cause – I'll be honest with you, I'm not really a major fan of security awareness anymore and I'll talk about that in a second. Cause there we were, I got in there, the people did everything right. Cause first I tried to like – someone was going out of the bathroom, I walked in the door.

Somebody ironically was walking in right behind me and they stop me. He's like, "Oh, can I help you?" I go, "I'm here to see so and so." And I knew this person would not be there and nobody ever knew where the person was so I'm like, "I'm here to see so and so." They're like, "Oh really? He went home sick today." I'm like I just spoke to him 15 minutes ago. He's supposed to meet me. He told me to wait in this like little alcove down the hall, which I knew was right across from the server room." So they were like, "Okay." They're like, "Well, I'm sorry. Please stay here in this area," which was right by the door, which had like a waiting area.

It wasn't a reception area, it was a waiting area and then like everybody's like, "Well, just stay here." I'm like, "Could I go sit in just –"They're like, "No, you have to stay here." Then like the woman went to get somebody that would – person came out and she's like, "So what do you do?" I'm like, "Well, I was supposed to talk to so and so about this." And she's like, "Really? What?" I go, "Well, I have this kid's TV show and we're trying to make sure it hits the right target audience." I actually am an Emmy Award winning children's television producer as well. But anyway, so I like just happened to use that and she's like, "Well, I'll have the person from the commercial side come talk to you." And then I'm like, "Commercial side? That's interesting." Because if you have a commercial side, you have a government side that's not on your website. So if you have a government side that's not on your website, it's classified isn't it?

So anyway, there I am and then like they come and get me. Everybody did everything right, which was so damn annoying. And there I am and like literally so then they're like – so they were all happy. And I'm like, "No, you're not perfect." I go, "Here's

the problem. I now know what doesn't work. I now know that you don't have a receptionist in the waiting area which means if somebody wasn't walking in behind me coincidentally as somebody was walking out, I could have possibly kept going. Also, while everybody was running around trying to get some guy on the phone that was not gonna get on the phone, I could have let somebody else in the door and you wouldn't have any clue and I could have just played stupid because it's really easy to play stupid these days." It's like, "Well, he looked like – he said he had to go check something out and I – why should I stop him? That's your job."

So anyway – and these are people who did everything right from a security awareness perspective because frankly security awareness is important. I didn't call people stupid, I think I said, "Before you can practice common sense, you have to have common knowledge." So you have to give people common knowledge so they can exercise common sense. That's a key thing because let me tell you the story that makes everybody laugh.

When I started working at NSA, I worked with this woman who's last name was Kirk, like Captain Kirk so I'm training her how to use the computer system. I go, "Okay, log on to the system. Now you have to log on to the database. Your database ID is your last name Kirk, K-I-R-K. Now enter your password, captain. C-A-P-T-A-I-N. And she turns around looking at me and hard go, "And how do you know what my password is?" I'm like "You've got to be kidding." And then she's like, "Captain's my password." And I'm, "Oh." And then she goes, "Oh and by the way, my father was in the Army. At one point he was a captain so there really was a Captain Kirk." I'm like, "Whatever."

So now here's this woman that sounds really, really stupid, but the problem was she wasn't a stupid woman. She was actually Cornell University graduate. She happened to also happen to be pretty smart and frankly was it her fault or was it the fact that she didn't know that that was a bad password to use. Frankly, people should be laughing at NSA security for not letting people know what a bad password that was. So anyway, that's part of the problem and going on with this other thing on why – I used to – you could read my books that say, "Security awareness is the most important thing." Frankly, I was so damn wrong because what you need to start doing is you need to start implementing fail safes for people. Just like that organization I mentioned.

Everybody did everything right, but if one person failed, I could be wandering around the facility that processes classified data. Likewise, by not having a receptionist there to control because they said, "Well, we're relying upon everybody to do everything right." And I go, "Everybody can do everything right and somebody else can go in the back door. Somebody else could do something else." Bad passwords, again, people will have bad passwords. People will write down bad passwords. People will do whatever else, but what do you do? You build in token based authentication like little one time passwords some people have.

There's a whole bunch – now how many people here are really in technology? Okay, so unfortunately a lot of people actually read that stupid thing in the program. So anyway, that's part of the problem. For those people in technology, you got to stop counting on security awareness because you have too many people to rely on security awareness frankly. Inside the organization I was breaking into, where I was "unsuccessful" at that moment in time, they had 30 people. It's really easy for 30 people to know everybody who's walking in and out of the place.

On the other hand, if you have a university with 30,000 potential users, you have people walking in and out of buildings like I was talking about. You can't control that. So if you can't control that, you've got to stop relying upon that. You got to start realizing that bad guys are gonna come at you wherever and however they can. For example, that first story I told where I'm walking in the building, what were the failings? Did technology fail in everything I did? The answer's no. I walked right by the guards. The guards failed, the receptionist failed. People held the door open for me. Once I was inside people left the systems logged on because that's just how servers are left. They're left logged on where anybody could go in and do something.

But there's other cases where I walk around buildings, I see passwords with sticky papers. I see pretty much everything. Anybody here a lawyer? Oh, sorry. But anyway, lawyers are the worst. Lawyers, you walk into their – they think my stuff is protected by attorney client privilege. It's like yeah, that goes really far. So they leave their most sensitive documents right on top of their desk.

One lawyer I was breaking into a major company and he had stacks of folders piled up so you couldn't even close his door. Then I picked the first one up off of there. It says this case is a nuisance lawsuit, pay them anything they want up to this to get rid

of it, however if they find out about this, pay them anything they want to shut them up. That's what's standing there right on these things. And likewise, let me tell you the first time I hacked into a university computer, and this probably – I didn't realize it was a felony at the time. It probably wasn't a felony at the time, there was no law at the time. So anyway, too late, statute of limitations, but I actually worked for all intents and purposes, I went to Syracuse University and I worked in the Admissions Office at Syracuse University for the Admissions Office where I was actually processing the paperwork that came in and putting it in folders and, of course, if they had an athletic name stamped on it, they got accepted no matter what anyway which is so nice to know.

So then what happened was turns out I had a computer system that I had entered things in and the computer system was always logged on and it turned – and it turns out I could look up anybody's records on that system. Did I need access to that? No, but it was so much fun to have. But there I was, able to look at anybody's systems because there it was. It was there, Admissions was tied into the Registrar for obvious reasons and if you had one menu, you had all the menus and stuff like that. So again, role base responsibilities.

Did I need access to my records? I probably could have figured out how to change it because I figured out everybody's passwords at the time was their initials. So if I knew it was registrar all I had to do was like figure out what their initials were, log in and then change all my grades. But I didn't do that which was really dumb of me at the time. Cause how people audit it? So anyway, I'm done. Any questions?

Female 1: As usual, Ira has a way of making the topic of security quite a very interesting one so thank you and thank you all to the panel. Any questions.

Male 1: Can the top five people of this session be scheduled for more sessions? Since it is such an important topic and it be announced as not just for IT?

Female 1: Very good, very good point. We will certainly take that back and maybe you can call Secretary Duncan and ask that Dr. Harris stay back and he can –

Danny Harris: Be glad to.

Female 1: He can assist us, but what I did want to mention is that there will be a birds of a feather session tomorrow afternoon at 4:45 in Asia 5 and we'll talk a little bit more about security and privacy issues and protecting PII data and there's going to be a checklist that we'll kind of go over so love to ask you to stay around if you're going to be here and any of you who will be here to kind of join that. So that's tomorrow. Any other questions? Could you use the mic please?

Female 2: This question is to the Department. How long do you think it will take before it goes into our participation agreement that we implement or institutions be enforced to actually have various programs that the first three spoke about?

Female 1: We're actually deciding that right now and on the outset it'll probably not be more than two years, but you will begin to see a number of initiatives. We want to work very closely with you all to ensure that we can assist in the process rather than just mandating so you will see us probably beginning this fiscal year to have that outreach.

Female 2: Thank you.

Female 1: Questions? Yeah. Can you use the mic please?

Female 3: Can I just talk real loud? Okay –

Female 1: No, you need to use the mic. They're taping it.

Female 3: Oh, okay.

Female 1: Here, why don't you take this?

Female 3: Along with that about the program participation agreement, is there any consideration being given to some of the software systems that we all use? For example, we're a campus management client, so is there any accountability that will be a part of that for data integrity with those software systems that we use and those third-party – I guess we're the client, but –

Female 1: Yeah, we are beginning the process, of course, hardening our systems internally, but we are looking at technology – is anybody here from yesterday's session, the software developer session? We're looking at technology that will help us reach out and actually begin the process of identifying who's coming in vis-à-vis your system so that is also coming. Any other questions? Sure.

Male 2: Ira, one of the things you said was that the bad guys are going to come after the easiest data to get and we work, in Financial Aid, we work a lot with both data that gets transferred, paper data that resides on our servers, what's the easiest to get? Is it easier to get into the buildings and get the paper or is it easier to get into the systems and get the data there?

Ira Winkler: It depends. Well, that's a lawyer answer. But frankly, I have to look at the thing cause honestly, depending on the situation, I can probably go into like – find the wireless access point and just hack into the network in the right building and see what the authentication is if you're using like some – like a lot of people think, for example, if you know WEP, that's completely unsecure even though everybody thinks wow, wireless encryption protocol, must be good. No, it's like give me a few minutes, it's down.

So that's one thing for example. The other thing is how do you treat your paper? Who has access to your buildings? Normally I would go ahead, I would do basic reconnaissance of the building. It depends because when somebody is going to break into your university, a lot of times – like you just saw a case I think in University of Central Michigan or something like that. You had a person who already had access to the University records and just used like login IDs and passwords that he compromised over a period of time, did a remote log in and downloaded lots of data.

Again, it really depends on who's doing the attacking and what methodology they're gonna use. The question is it's like eventually somebody will get it, but how hard do you make it because I use the analogy – it's kind of like somebody keep popping their head up over a fence. If you just rely upon preventing a compromise, you're gonna fail. You have to make sure you have the right sort of detection capability in place. Like if you see a lot of accesses from an account that shouldn't really be accessing that much data, you should know to lock them out, or investigate.

If you see somebody like trying to break into the building and you see people wandering around, take their name and at least find out who they are so if you see that person again – because what happens are when I investigate crimes, I find that it's not just one case, that there's lots of things that if they looked, they could have identified the person months in advance. The benefit is a lot of criminals are really stupid and take a lot of time. I'm very good at figuring out how to get in and get the data really quickly, but most criminals, if they're gonna compromise you remotely, they're

gonna just use computers and it's really easy to get into the university. But then the hard part is figuring out the right computers to break into. And so what they're gonna do is they're gonna perform reconnaissance and search around the network.

Does your university have technology in place to look for potential intrusions or misuse of the network to figure out if somebody's scanning your network and doing things like that? So if they're gonna compromise you technically, they'll go in like that and do that.

Gene Spafford, he's from Purdue University. He's like one of leading professors in computer security. He says, "Universities don't need firewalls cause firewalls are meant to keep the bad guys out. We already have them inside." That's his quote. And so you got to look. Are you looking for students misusing and abusing which is this case of University of Central Michigan. Likewise are you looking around? Do you have good physical security in areas where you have PII types of data? Cause, again, it depends on the criminal which tactic they'll take.

Male 2: Good, thank you.

Female 1: Any other questions? I think what you're hearing, despite what Ira says is that security is a comprehensive solution. There are many, many different facets. People do matter, culture is very important, training is extremely important, technology is extremely important and none of those can stand on its own. So it has to be a comprehensive solution. Monitoring is extremely important and it has to be continuous monitoring so all of those, I think, will make for a comprehensive and a good security program.

I want to thank the panelists. Thank you for your time. Thank you for your insights.

[End of Audio]