Danny Harris: My name is Danny Harris, and I am the CIO at the U.S. Department of Education. Welcome to this session. Let me begin by thanking FSA CIO Richard Gordon, and Bridget-Anne Hampden, the deputy CIO, and the entire FSA family for inviting me here to talk about issues that I believe represent the most critical IT security and privacy issues of our time. I believe the most significant thing that you should walk away with as practitioners in the field, whether you're in IT or any other line of business, I think the most significant thing that you should walk away with is you will never, ever get ahead of cyber criminals. If you're staying awake at night attempting to get ahead of the cyber criminal, go ahead and take a pill or two and just go to sleep. It's not gonna happen, and I think you will go to a number of sessions like this where that statement isn't made, and I think what this is all about is reducing the risk footprint. You will never reduce all of your risk associated with privacy, associated with information assurance, associated with IT security, so what you really need to do is reduce the footprint, and so we're going to talk about a subset of that today.

Before I get started with my presentation, what I'd like to do is introduce you to the person who I've already been told looks much better than me, several folks have already mentioned that and it looks like they have good eyesight, Sheila Colclasure. She is the privacy and public policy officer of the Americas for the Acxiom Company. As Acxiom's privacy and public policy officer for the Americas, Sheila is principally responsible for managing the fair information practices and compliance, client support, and external policy setting of a publicly traded information management company with annual revenues in excess of $1 billion. Founded in 1969, Acxiom is headquartered in Little Rock, Arkansas with locations throughout the U.S., Europe, Australia and China. Acxiom integrates data, services and technology to create and deliver customer and information management solutions for many of the largest and most respected companies in the world.

Sheila's primary areas of focus include monitoring and coordinating enterprise-wide compliance with legal regulations. As part of her role, she has developed and implemented an annual privacy audit function that is widely regarded as the best in the industry. She advises elected officials and regulators on privacy issues and privacy legislation. She also works with Acxiom's clients and industry members to show them how privacy compliance is an essential component of their overall business strategy and how it can be competitive or be a competitive advantage for their business. So, Sheila will follow me after I do

my very, very quick presentation.

So, protecting students' information from unauthorized access. Let's first baseline on some definitions. If you search what data breach and PII is on the Internet, you will probably get several thousand hits, and so what I wanted to do initially is just to kind of give you some laymen definitions for those two terms, because we will be talking about those two areas. So, what is a data breach? It includes the loss of control, compromise, unauthorized disclosure and unauthorized acquisition, access for an unauthorized purpose, or other unauthorized access to data, whether physical or electronic. Very critical. And what is PII? For the most part, PII is information which can distinguish or trace an individual's identity. It's information that can uniquely identify an individual, and what's very important about PII is on the surface we all think of Social Security number, but there are a lot of other data elements that if you put them together they can uniquely identify an individual.

So, data breaches, in the news, both on the private sector side and on the public side. We know that a Sony website was breached allowing access to personal information belonging to over 1 million Sony customers, October 2011. Very annoying. I couldn't play with my PS3 for three months. I mean that's where I dealt with my stress, and so that was very painful to me. Google, June 2011, Chinese hackers infiltrated Google's Gmail system and broke into hundreds of accounts, including those of senior government officials, military personnel, and political activists. On the education side, closer to home, closer to us, Ohio State University. Data breach costly for Ohio State victims, 760 individuals. Expected to cost the university $4 million. UConn, personal information exposed in a data security breach, where a hacker was able to access the Huskydirect.com customer database, affecting 18,000 records, and then finally, our very own FSA, private financial information belonging to as many as 5,000 college students was open for viewing on a federal government student loan website. Very, very painful.

And so longitudinally across the years, what do the breaches look like, from 2005 to 2011? Here are some numbers. We see that in 2010, 73 reported breaches, 1.5 million records, and what's terrifying, what is absolutely terrifying about this slide is this is what was reported. This is what was reported, and so let's talk for a second about the other scenarios. There are other scenarios that people know about that they didn't report, and then there's the larger population. Let's make the assumption that there are many

more breaches that we don't even know about. No one is hiding it; we just don't know. That's terrifying. Here are some facts that just blow the mind. Who's behind data breaches? Forty-eight percent were caused by insiders. Forty-eight percent. So, if we split the room almost down the middle, half of you are responsible for breaches in your organization. Well, maybe not half of you, but it's still a staggering statistic.

Eighty-five percent of attacks were not considered highly difficult. Sixty-one percent were discovered by a third party. How embarrassing is that, by a third party? Eighty-six percent of victims had evidence of the breach in their own log files, and when do you think they reviewed those log files? After the breach was discovered. That's embarrassing. Ninety-six percent of breaches were avoidable through simple or intermediate control, so it takes me back to the very beginning of my presentation. This is not about building very, very sophisticated deterrents. This is about prioritizing and figure out, "How big is our risk? How big is our risk footprint, and what can we do in terms of people power, money power? What can we do to reduce the size of that risk footprint?"

And so what is risk? It comes in a number of categories, and this is not a comprehensive list, but identity theft: the FTC estimates that as many as 9 million Americans have their identity stolen each year, 9 million. These are huge numbers. Business and financial security: trust and confidence in the market place and in U.S. companies, and this is profound because more times than not, when you go to a presentation on IT security, when you go to a presentation on privacy or information assurance, there's typically a discussion on dollars and cents, "How much is this costing Company X? How much is this costing Company Y?" but what we really should be thinking about, and certainly at FSA and the department, our bigger concern is, "What does this do to the trust that the American people have in our ability to manage their money, their business processes, and their identities?" and so that's much more important to us.

Social interactions and norms: adults and children are willing to share information with people they don't know. Not all social media sites protect information. Forty-nine percent of teens who use social networking websites use it to make friends with people they don't know. How can you actually make friends with a person you don't know? I mean that's kind of odd. I mean I know a lot of people and they're not my friends. So, that's kind of odd, but it's staggering. Cyber stalking: a technology-based attack on one

person who has been targeted, whether it's for harassment, embarrassment, to get at their assets, to harass their family, or just to strike fear. So, I could go on and on and on, and certainly Sheila, when she gets up here, she's going to probably also share some staggering statistics with you, but that's not really what this presentation is all about. This is more about, "What do we do? Okay, Danny, you said that you don't have to have $1 trillion to fight the criminals; they'll always be ahead of you. Well, then what do we do?" So, I'd like to share with you very quickly what the department is currently doing, and second, what our near-term plans are, and then, more importantly, I'd like to talk to you about what you can do, some tips that I have for you.

The first thing, if you are an executive, if you are a manager, if you're a decision maker in your organization, the number one thing that you can do is hire the best and the brightest in this field. As the CIO of the department, IT security information assurance is not my core competency. I knew that when I took over the role, and so what I did was I went out to hire the best IT security information assurance individual that I could find, and she's here today, Michele Iversen. So, if you get a chance to speak with her, please do that. I think she's presenting at another session. So, we hired a new chief information security officer who is building – listen very carefully to this one – who is building an IT security information assurance that supports privacy program. In other words, don't allow the professional to walk in and start chipping away at problems that you know about. It's not about just coming in to say, "Okay, what's paining you?" It's about coming in and building a program. You can't defend on specific issues. You have to have a program because the problem is so multifaceted.

Number two, we established a robust, multi-factor authentication for internal and external authentication. If you don't have two-factor, if it's not in your near term, you need to revisit your strategy. Enhanced continuous monitoring program enabling real-time automated auditing. If you have two-factor, if you have firewalls, if you have all kinds of gadgets and gizmos that are supposed to protect you but your monitoring isn't automated, you're still behind the eight ball, and so that's one thing that Michele brought in-house, continuous automated monitoring. We deployed full disk encryption for mobile devices. We significantly enhanced our cyber security awareness program, and, quite frankly, the item that costs the least but returns the biggest dividend is building a strong cyber security awareness program. Why? It takes it us back to one of the earlier bullets: 48 percent

are insiders. Some of them are known offenders, but others are just maybe stupid. No, that's not a good word.

Audience: *[Inaudible comment]*

Danny Harris: Okay. Thank you. Thank you. Careless. So, we need to make them less careless. That's our job, and that will pay high dividends, and, quite frankly, it doesn't really cost that much money. There are all kinds of best practices on how you build a strong security awareness program. Finally, we partnered with the chief privacy officer and the Privacy Technical Assistance Center to make security program more holistic. The bullet that's not on here that's really critical is we've joined forces with Richard Gordon and other folks throughout the department to make sure that the security program is holistic, because it doesn't make sense that if we have security on one side of the fence but we don't on the other, we're not secure, and I'm embarrassed to say that it probably took us 20 years at the department to realize that. That's embarrassing, but the good news is we realize it.

What have we planned for the near future? We're improving systems engineering processes to build security into the system and design. For those developers in the room who came to the developers conference, and Richard and I kicked that off, one of the major things that I talked about that we still don't do today is when we start a large implementation project, the thing that we don't do is we don't bring those IT security specialists to the table on day one to ask the question, "Here's what we're trying to do. What are the known risks? Here's what our architecture looks like. Poke a hole in it. Here's the code that we're gonna use. Do you know any known issues with that coding _____?" We don't do that, and that's easy. We're actually paying them to protect us from the very beginning but, typically, what we do is we wait until we've developed, we've built the architecture, and then they come in and they do an audit, and that's when they tell us, "You've got some holes here." That's backwards, folks. That's backwards. We're gonna implement data loss prevention tools to enforce information sharing policies and prevent inadvertent disclosure, and we're going to establish a mobile device management strategy. My near term is the next 12 months, just to give you a timeframe.

So, what can you do? You might say, "Well, Dr. Harris, we don't have much money." Yeah, you like the slide, huh? Let's make sure that face isn't your face in the future. So, what can you do? Number one, implement multi-factor authentication. Show of hands: how many organizations in here are either doing two-factor or multi-factor, or are on the verge of doing multi-factor? Okay,

good. Interestingly enough, last year, if I had asked the same question, we may have had two hands, so we're growing very, very quickly together. MFA should support web applications and should not require client-side software. When interfacing with federal agencies, ensure identification and authentication mechanisms are compliant. Support the National Strategy for Trusted Identities in Cyberspace.

Deploy best practices. Folks, they are everywhere, and guess what? There are folks all over the world dying to provide those best practices for you. There are many vendors who, yes, they want to increase their revenue, but more times than not they're willing to come and talk to you for free on the best practices that you can deploy to actually secure yourself better. These are basics. Use a firewall. Install and maintain anti-virus software. Install and maintain anti-spyware software. Use spam filters. Set your software to auto update. How many of you have installed it but it's been years since you've updated it? No one will raise their hand, but I guarantee you there's a large number of people who have done that. And the last bullet here, build security in. Again, developers should use emerging tools, rules, guidelines at the very beginning of the implementation process – not in the middle, not at the end.

This is a takeaway for you. I think the slide deck is going to be posted on the website eventually, so you'll have that, and there is my contact information. Again, what I'd like to leave you with before I turn it over to Sheila is build a solid program from the ground up, and prioritize. Don't worry about the money you need to do it. There are a lot of things that don't take a lot of money, but build a robust program. You first have to figure out where your weaknesses are before you can start working on them, so do solid assessments. I'll turn it over to Sheila.

[Applause]

Sheila Colclasure: Well, let me add my hello and thank you to both Richard and Dr. Harris. That is a tough act to follow. I don't have near the booming resonant voice or command, but let me give you a little bit of why I'm here today and why Acxiom. Does anybody know who Acxiom is and why this is such an important issue? As a billion-dollar information services company that's been around for 40-plus years, the billion dollars of revenue we create each year is created through handling our clients' data, personally identifiable data mostly, or data that we compile on individuals, mostly personally identifiable, and we do this everywhere in the world, and the rules everywhere in the world are very different, so for us,

handling massive amounts of data. In fact, in one of our – we have I guess down in Conway, Arkansas the largest non-governmental data installation in North America. We have 16 acres of raised floor. It's said that if a bomb hit that facility and the redundant facility, then banking in America would stop for a few weeks.

So, this is a very critical issue for us, and as we've worked through different industries over the 40 years handling our clients' data. We've had to become very nuanced on what their obligations are, what kind of data they collect, how they want to use it, what's available, what's not available, what laws they're obligated to, and then we have to architect very sophisticated systems, not just to solve the business problems, but also to address the stewardship, the security of the data, and to bake in the policy, the appropriate handling and use. So, for Acxiom, we don't just handle client data but we compile data, and we have a fiduciary responsibility over that data, too. So, we've grown up doing it, and there's one thing that we absolutely know, is we live in an information-based economy and data is gold. I suspect in about three to five years it's gonna be a reportable asset on your SEC filings. It's a big deal, data, and, as gold, it's a very hot commodity.

Do you know the street value of a set of identity credentials? About $150.00. So, if you get 1,000 records, that's a big deal to an identity thief, $150.00 per record. But it's in the news, and I throw this slide up here to tell you that these issues are in the news and that it's ubiquitous. So, all of the privacy issues, not just the security issues, but the misuse issues; not just unauthorized access, but all of the privacy issues kind of swarm in together. The media thinks about them the same. They write stories about them. They don't differentiate or give you credit for using it right versus not keeping it secure. So, when you have a privacy incident, know that all of the pressures that have been heaped upon the subject of appropriate collection, use, sharing and protection are all attached to the data that you collect and that fuels your business.

These are actual quotes out of *The Wall Street Journal*, "Vast data gathering … used to discriminate the services that companies and government offer citizens." "Growing concern on Capitol Hill about the ability of organizations to keep the data secure." One of my favorites, Anne Toth of Yahoo, she's now moved to Google a few months ago, does anybody know Anne? She, at Yahoo, was their chief trust officer, and she made a statement in an interview to *The Wall Street Journal*, "There's no way at Yahoo that we could know all the tracking technology that gets loaded onto a user's machine when you come to the Yahoo website. There's no

way that can be known." Each of your websites, if you have a website, I promise that you've got all sorts of tracking and collection technology that your technologists load on there, and all of that data comes in and it gets put in tables, and there are actually layers and layers of rules that apply to all that different data, and when your technologists use it, or grab it or scoop it in and put it in a database, that too must be accounted for.

The Wall Street Journal themselves, they wrote all of this. Do you remember this privacy series that's still ongoing? It was really, really hot several months ago, and they're kind of trickling out the stories right now. Did anybody read all *The Wall Street Journal* series? If you go to the Wall Street website, they made much ado about tracking technology, and on their website I think they clocked in at 356 tracking technologies if you go to their website. But it's big stuff. It's made it to mainstream press. This is one of my favorites, "Customer data is an asset that you can sell. It's totally ethical because our customers would do the same to us if they could. Sounds fair. In Phase One, we'll dehumanize the enemy by calling them data." So, you think about this and you think about it's out there in the funny papers, so these are real issues.

My one takeaway for you today is when you think about the data that you steward, the stuff you're collecting straight from the individual, the stuff that you overlay – maybe a credit report, maybe data from Acxiom – all of that data comes with some emotionality. So, we know that the media has made a lot about it, we know that it's made mainstream and the funny papers, and we know that it's a very, very emotional issue. An extract from a great deal of consumer research is that consumers feel like they've lost a lot of control. We also know that they don't appreciate that we live in an information-based economy, and one of my responsibilities at Acxiom is the lawmaking piece of it. I spend a lot of time in D.C., and happy days out in the states at the different state legislatures, and those move at the speed of sound. You can have a piece of legislation drop in a state on a Monday and get signed into on Thursday, and all of this is very emotionally driven, and your takeaway today, the one I'd like to leave you with, is remember that emotionality comes with all the data that you collect, so you have an obligation to account for that emotionality.

Now, there are a few drivers and trends that I would like to call out. Number one, we do live in a riskier world. Has anybody in the room been a victim of identity theft or fraud? Yeah. So, if you think about the harms, there are real harms and then there's

perception of harms. What we know is both of those, if you actually get harmed, it's pretty awful, but the fear of it will drive behavior and certainly drive attitudes. Identity theft, of course, occurs on a continuum. When you think about identity theft, on one end you have credit card fraud, where you have a fraudulent charge on your card, and on the other end of the spectrum, you have true identity takeover, where someone has gotten your identity credentials and they bought a car, they've taken out a mortgage, they got arrested and used your identity.

One of the newer ones is they've gone and gotten some healthcare, and then you show up at the hospital a week later and they say, "I'm sorry, Dr. Harris, you just had your pancreas operated on." So, it happens. Another one of the drivers, and this is really hot right now, there's harm, there's perception of harm, and there's surprises. You don't want to surprise the consumer. Unfortunately, with the escalation and the speed of innovation, there are new data-intensive collection technologies that often are invisible to the consumer, and then, when they hit the light of day, when they see the light of day, it surprises everybody and it turns into an incident.

There's a big blurring between anonymity, or anonymous data, and personally identifiable. I think we could all out in the room what we believe today is personally identifiable. Clearly, my name. A sensitive piece of data would be my Social Security number, my mother's maiden name, detailed information, personally identifiable information about my children, but there's other data that in some countries is actually personally identifiable or considered or regulated as such. A couple of countries in Europe regulate IP address as a piece of PII. We don't yet in the United States, but when you think about anonymous data, a lot of the stuff that we collect on our website when the individual who's shopping your school or university online then enrolls or inquires and they make themselves known, oftentimes what you do or your technologists do is all of the cookie behavior that's been watching somebody show up. You dropped a cookie, they showed up once, you see them, they come back again; you might optimize your website for a much better experience or to pull up the most recently viewed.

When they convert and they make themselves known, they key in their name and address or their e-mail only, you will associate, or your technology people will associate those pieces of data. Now, you may not know this, but you have to have a very express statement in your privacy policy before that's illegal to do, all

right? In many instances, and one of the things that I and my team have the joyful privilege of doing at Acxiom, is when we source data, we read each and every privacy policy under which the data is sourced, and I'd say roughly about 90 percent of all privacy policies have a statement about passively-collected data, technology-collected things like cookies, beacons, pixels, tags, footlights, spotlights, IP addresses, device IDs, device fingerprints, and they make a statement that it's collected and say that it's anonymous and will not be joined with PII. In practice, most of the time when the individual converts, we actually do that. So, you need to think about those sorts of things. When that sees the light of day, that will turn into an incident.

We've almost moved into, and I think we're probably already there, some of the dots are not connected, what I think is the surveillance society, and I'm gonna talk a little bit more about that in a minute. But I want to give you a few statistics to really drive the point home that people care about this issue behaviorally and attitudinal, and a couple of the statistics – 64 decided not to use a site because they weren't sure how data was gonna be used. That's behavioral. They clicked off the site. They got a little skeptical. Maybe they read the privacy policy. Sixty-seven decided not to register or shop because the privacy policy was too complicated. Twenty percent of the population believes they have been a victim of identity theft. So, whether or not you've been identity takeover or you've had a card charge, a fraudulent card charge, a significant portion of the population believes they've been a victim, so that makes them very sensitive.

I want to call you down to the bottom statistic here. Dr. Alan Westin. Does anybody know what – he's called the grandfather of privacy. He's been studying this. He's a prophet. Columbia School of Law, and he's been studying the issue for a very long time, and he's assembled about 20 years worth of statistics on how consumers feel about privacy, and he breaks consumers down into three buckets. You have the unconcerned, and I think those are snowboarders in Aspen, and I think they're off the grid, and then you have the pragmatists, and the pragmatists are those people who understand, "I'm gonna give you my data in exchange for value." There was a great bit of research done in Washington, D.C., I guess about five years ago, it was on a hot August day outside the Metro Stations, and there was some survey people with clipboards standing outside the Metro Station asking passersby, "Can I have your personally identifiable information?" People were saying, "Heck no," and worse.

Then, at other Metro Stations, they had a freezer carton rolly thing of Dove bars, and they were holding up the Dove bars and saying, "Dove bar in exchange for your personal information," and they were asking for Social Security number, and people were saying, "Oh heck yeah," and they were giving their name, their SSN, and, in certain instances, "If I give you my mother's, can I have two doves?" So, that is the pragmatist, you know, "I trust your brand, you're going to give me service, and I'm gonna give you my information in exchange," right? Pragmatists. But 34 percent of the population is the fundamentalists. They really care about the issue. They're gonna test you, they're going to leave you if they don't trust you – this is what Dr. Harris pointed out. Trust is so essential for your brand. And guess what? They're going to report you if you violate. They're gonna do something. They're gonna call the state AG, they're gonna call the media, they're gonna do something, so 34 percent of the population, that translates to 34 percent of the folks that you deal with; maybe not the student, but certainly their family. So, we need to be mindful of that responsibility when we're building our systems to keep the data secure and protected.

In the surveillance society, I just want to point out to you kind of where we are and where we're going. Really, really hot right now are apps. I mean we all have smart phones, or I like to call them hip computers. The penetration here in the United States has just topped 40 percent of us carry hip computers. Do you know what the penetration is in Japan? One hundred percent. I was at a few months ago a _____ event on mobile. I was a speaker. I wasn't elite enough to be an attendee. You have to be a CEO to attend, and the CEO of DOCOMO was there, and we were in a session. It was an innovation session, and, as a speaker, I got to attend and it was just a fabulous, mind opening experience. There was a guy, an innovator who was demo'ing a prototype of what's coming for all of us.

Our hip computers are gonna change from on our hip to these wild things that go across our eyes. We'll see through them, but we'll have – you know, there's movies that are made. The little visual that plays here, and you ask for some GPS via voice command, and this thing comes down over your mouth, and this guy had it on. He was demo'ing it, and then, in the side, your peripheral vision, there's the GPS map and you just walk along and follow it. I raised my hand and I said, "Well, how do you breathe?" and the CEO of DOCOMO said, "Oh, in Japan," and with greatest adoration for the Japanese and their accent, and I mean that, he said, "Oh, in Japan we have a special app. You breathe quite easy. It ionizes the air as

you breathe," and I thought, "Boy, if I could get an ionizer and a germ filterer, I'd be wearing that gadget all around town." But it's coming, and it's not that far away. So, apps, this is the way, and if you don't already have an app for your school and for the student aid, the application process, if you don't yet, you will, and so you need to be very, very mindful of the kinds of data, the quantity of data that is collected via your app, and what your app provider. So, this is another very, very important thing that's happening today that you need to be very careful about because you've got to make sure that that data is also secured, that you've thought about it and planned for it.

Device fingerprint. Does anybody do this as part of the authentication process today? On your phone, or your hip computer, this is specific to smart phones, there is a device ID that's specific to the device itself. But, also, many websites have gone to authentication where they take some data metrics, not just the device ID, that's one piece, but the fingerprint of the phone – what kind of browser, how many browsers, how many fonts what fonts – all sorts of things, and they build a fingerprint on your device, and that's here today. So, when you think about anonymous versus PII and what kind of data you're stewarding, know that the definition of PII remains fluid, and you've got to plan for the future.

Precise GeoLocation: hot, hot, hot. Sensitive. Perhaps more sensitive than an SSN, right? You're gonna all want this and your app will probably want to use it, if you have an app for your school. Precise Geo is so important. When people are proximic to your school, all of a sudden you become very relevant, so you're gonna care a great deal about it, but in the Precise Geo, it's going to be regulated as a sensitive piece of data in the very near future. It's regarded as such today and it will probably become a piece of law. Now, you don't do this, but let me tell you why it's sensitive, just to really drive it home. Let's say Starbucks, one of my favorite brands, every day I drive home past a Starbucks, and I drive home, I've got to pick my children up at about 5:30.

So, I'm driving past, I pick them up, and we drive on home, and they would love a cocoa and I probably would love some sort of – so, on the Starbucks app, I get a little Geo location a few miles before Starbucks because I said, "Yes, you can know my location." Well, guess what's next door to Starbucks? It's a liquor store. So, every day, I drive by Starbucks at about 5:35 and I drive by the liquor store at about 5:37, and guess what? I stop. Every day at 5:37, I stop, not at Starbucks, but at the liquor store, and I make a

purchase. Over time, when you have Precise Geo, plus the amount of time, plus the purchase behavior, it becomes extraordinarily sensitive, and the scenarios can go on and on and on. So, you think about the sensitivity of Precise Geo. There's a great fuss about this, not just here in the U.S., but virtually everywhere around the world.

Does anybody know what HTML5 is? It's a new functionality that's coming out, HTML5. It's gonna replace the need for Adobe, let's say. Your HTML, it'll be HTML5, and it will offer you absolutely every functionality that you could ever want, to read any software, play any video on the Internet. Very interesting, very useful, but here's the deal. It's going to capture everything you do in one spot on the Internet, so this is another very escalating thing around privacy. There are already sniffers and listeners. Many of the brands in this room use these today. Some of you are our clients, so I'm intimate with your information practices, and a sniffer is something that goes out on the Internet and looks for discussion about your brand, and a listener sits on a pipe and listens to see what is talked about, if it's positive or negative, and builds a report around it.

Meters just clock the traffic. They exist today. So, think about all the digital dust that's created by all of us users, and if you can collect that, if you have meters on your pipes, think about closing the loop and how your data stores begin to build, right? When you attach that to PII, the potential for harm, the perception for harm, the perception for a violation of dignity grows in magnitude, so your fiduciary responsibility to protect and control access to that data grows exponentially. High tech, this is a great example of what's coming our way in the future, not very far away. Your medicine will come with a little RFID chip, and when you swallow the medicine, it will go down and be absorbed into your system and the RFID chip will read and clock the absorption and the efficacy in your system, and upshoot that data to the Cloud, and it will go back to your doctor. You almost won't need to go in because he'll know how effective the med is being and what your uptake of it was. That's what's coming. It's been developed. It hasn't been rolled out yet except for test groups, but it's here and it's soon.

In the world, there's going to be a magnification of extraordinary scope and scale of all of our connections to the Internet. Everything, all the devices, your refrigerator, your stove, your lights, your heat and your air, your digital television, everything will have a connection to the Internet, and you think about the

magnitude of data that's being created. Placefulness coming your way, as well. This is the future of things, that you will be so known that when you are in a place, you will be known. It's sort of like there's a movie that used placefulness, with Tom Cruise in it. He was walking through the – what was it?

Audience: *[Inaudible comment]*

Sheila Colclasure: Yes. He walked through the mall and he was recognized, and his last purchase, of course he had his eyes replaced, but the last purchase, and they tried to upsell him and asked how he liked his purchase. That's actually coming to all of us. So, "Your customer data is worth a fortune. I'll find you some buyers if you give me 25 percent. What about privacy? That's not a problem. I never use my real name." I want to explode some myths for us all in the room today. When you think about your stewardship of data, you really need to bake it into your culture. It's as Dr. Harris said, it's everybody's responsibility. It's not just the IT, and it's not just about a security breach. Remember, everybody thinks of privacy issues in a very ubiquitous fashion. It's all the same. If you have a mistake, it's a mistake. It's an incident. So, it's not just about external intrusion. It's about things that happen internally, as well. Forty-eight percent of issues come from the inside. It's all about identity theft. It's not. Most don't result in identity theft, most issues don't.

System security is an essential, but it's not enough. It really has to be a policy program education process that you bake into your organization. You need to have a governance plan and a response plan. If you wait until you need a response plan, it's too late. I don't know if you guys know this: do you remember 2005, the year of the security breach? That's when it all exploded on the media. Do you know when the very first data security breach law was passed and in what state? The state of California, and it went into effect in August 2004, and guess what? Acxiom Corporation was the very first company in the nation to trigger that breach law. The law went into effect in 2003 on August 1, and we got a call – I did – from the FBI on August 3, and they said, "We've just raided the bedroom of a young hacker named Daniel Baas in Cincinnati," because he online blogged in the hacker community about threatening the life of the president.

So, they raided his home, and in his bedroom – this was a 23-year-old kid. In his bedroom, we found these tapes, and they said Acxiom Corporation on it, and of course we were horrified, and I sent our general counsel, Jerry Jones, and our former FBI security guy, Jamie, up there to interview the guy, and he was, he was a

young hacker, and he had stolen the Acxiom data for bragging rights. He actually worked for a client of ours, and while he was in a pick-up/drop-off FTP server servicing the client with client credentials, he ran a de-encryption program and cracked an encrypted password table, got in there and stole a bunch of client data. He didn't do anything with it, it was a wholly contained incident, but nevertheless, he downloaded massive amounts of data and put it on files and stored it in his room, and bragged to his girlfriend and his mom. It was, "Look what I did." He wanted to impress.

Anyway, I think he spent about three years in prison. We prosecuted. But, as a result of that, we developed an incident response plan. Actually, as soon as we got word from the FBI, immediately, within hours, we had a war room, we'd call the press ourselves, we called the Federal Trade Commission. The only law was California. We called the California state attorney general, and over the next weeks and months, I spent a lot of plane time going back and forth between the FTC and the California state AG and different clients, because this all involved client data. Now, you know, our client said we handled it better than anybody they could have imagined, and it really established, reinforced their trust in us as a good partner. But I'll tell you, you've got to have a plan.

Does anybody know what happened at ChoicePoint in 2005? A lot of my friends worked there. They were a competitor of ours. They don't exist anymore because of this, but in 2005 they had a breach of about 161 records. I don't know if that's exactly right. It resulted in identity theft cases, and some guy at Kinko's filled out paperwork like he was a client. So, he filled out all the paperwork, but they didn't do vigorous enough credentialing, and so the guy got some identities and he committed identity theft with them, he caused some harm, and it was 161 records. Anyway, what they did wrong is they didn't have a plan, and when it hit the media, they waited five days. They refused to talk to the media for five days, and then they finally _____, "Okay, okay, okay." Bad press, bad press, bad press. "Okay, we'll talk to you." By then, it was too late. The tide had turned.

Then, because there was only one law in place in California, they said, "Well, we'll make notice in California, but we don't have to anywhere else." Second mistake. Seventeen different state AGs came together and sent them a letter and said, "That is unfair. We're gonna get you. It may be down on a state security breach statute, but we're gonna get you for being unfair and deceptive

because it's not fair to our citizens if you don't give notice in our state, as well." Of course, they did, but it was too little, too late, and this is what it cost them. You'll see this in a later slide, but it cost them. The Federal Trade Commission got them for a $15 million fine, and that was the least of it. Just to get their consent to _____, they spent $43 million, just to ink the Consent Decree and pay the fine. Then, they had to go back and re-credential 6,000 clients, and they had 20 years of biannual audits, and a remediation plan. So, it's very expensive. Even for 161 records, it's a big deal. As a result, of course they couldn't survive, and they got chopped up, sold off in pieces, and they're now a thing of the past.

I also want to call out does anybody remember what happened to Epsilon a few months ago? Epsilon had a breach, and it didn't involve any sensitive data. It involved e-mail addresses, which are not sensitive, and a few years ago, there was even a debate whether or not they were personally identifiable, but of course they are. But it was a lot of e-mail addresses, and it was a hacker, it was somebody who breached their firewall. The same people tried to breach us, and because of our incident in '03, we have very aggressive security, so we can't be penetrated, or at least this guy couldn't get in and get us. They got got, and it was decimating to that line of business for them, and they're still recovering. They lost clients, they've lost revenue, they had to do a lot of triage and spend many millions, so it's a really big deal. Law and public opinion are formed about our obligations to keep data safe, and it's only becoming more punitive.

So, a little bit more about the cost. Do you remember what T.J.Maxx, they had their big data breach? They ended up having to declare $168 million write-off. Huge. ChoicePoint, we just talked about. Eli Lilly, I have permission to retell this story from Stan Crosley, one of my personal friends, the chief privacy officer of Eli Lilly. Does anybody remember what happened? This is another flavor of breach. Well, Eli Lilly, pharmaceutical giant, they had a Prozac newsletter that people signed up for, and when they signed up for the newsletter, there was a privacy policy. Inside the privacy policy was a security statement, and the security statement said, essentially, "We will not share your identity with anybody else. Trust us." After a few months, there were only about 760 subscribers, and then it was too much internal effort and cost and resource, so they were gonna retire the newsletter and post the content on their website.

So, Stan crafted a retirement newsletter and he had a Cornell

graduate, computer sci, 4.0 girl who was the administrator of the program, and she prepared the e-mail, and she got ready to send the code, and there was one paren missing from her code string, and that one paren caused all 761 names to populate the two instead of the BCC, and she hit Send and she went, "Oh!" She ran upstairs to Stan and she said, "Stan, Stan! Oh my gosh, do you know what I've just done?" He was like, "Oh my gosh!" They got three phone calls, three complaints, and Stan talked to all three. The first two said, "Oh well, I understand how mistakes can happen. Okay, okay." The third one said, "That's not okay. You promised to keep my identity secret," and Stan was like, "Well, it's really just your e-mail." "I don't care. You made a promise. I'm going to report you to the Federal Trade Commission," and they did.

And so Stan, Eli Lilly, got a Consent Decree, and it took him eight months to negotiate, because it's a very intense negotiation with the Federal Trade Commission, and to ink his Consent Decree, it cost him – just the negotiation and the triage part – $18 million, and then he, too, had 20 years of audits and a remediation plan. Now, the good news is – here's the good piece of that story – he developed a control, a program, a data governance program, a training program for all the employees, and all these really good control protocols, and a few months later they had another one. It didn't make the press, and the FTC came in and said, "Oh, but you had a good governance program. It was just an error, but you really tried. You have a documented program and plan in place, so get a pass on this one." So, it's very important that you actually address these things.

The average cost per record in violation is about $210 million. So, it happens a number of ways. It can be a system interception of a wireless transmission without a firewall. It can be those wireless pay systems. It can be an inside job. Call center audio files, one of my favorites. *The Boston Globe* used some old account documents. They took the paper files, flipped them over and wrote, "For pickup," on their distribution bundles, and when you turn them over, it had people's names, addresses and SSNs. So, paper really counts. You've got to be very accountable for that. It's the data that we all know. Identity thieves do this many ways. I think Dr. Harris covered it best, but I'll tell you social engineering is the one I've seen most effective, and the buying of personal information from the inside.

They use it to commit a number of harms and acts against you, but remember, it's not just for the IT folks, it's for everybody. It goes

to your brand, it goes to trust; putting a good governance program in place to protect and secure really does protect your brand. Remember that all of these risks evolve, so if you aren't constantly evolving your practices, you're not keeping up. Make your employees aware. This is what I tell my employees at Acxiom, "It's not gonna be me in the orange jumpsuit, because I don't look good in orange. It's gonna be you." Sensitize your employees to watch for bad behavior. They're the ones that are working elbow-to-elbow, so sensitize them, "If they see an issue, raise a hand."

A number of to-do's: build that data governance plan, assess needs and purposes for all of the data that you collect, and all the mediums and all the channels via all the technologies, and understand exactly why you need it. The more you collect, the greater the fiduciary responsibility. Don't keep what you don't need. Monitor, monitor, monitor. It's not a question of if, it's a question of when it will happen, because as Dr. Harris pointed out, there's many that go unreported, and think about it. We didn't even start hearing about it until 2005. It doesn't mean it never happened. Have a plan, keep it in writing, keep it up to date.

Seven rules to live by: you have more sensitive information than you think you do. Data in transit is data at risk. Encrypt, encrypt, encrypt. Employees are your greatest risk, unfortunately, either because they're purposeful or they're just careless. Vendors are your second greatest risk. At Acxiom, we have about 85 security audits a year, so you should do that with any vendor that you have. Overreact if you have an incident. Be very helpful to the stakeholders. I was in a hearing right after the ChoicePoint event, and the state of California and the judiciary committee were having a hearing. ChoicePoint got up on the stand and they said their piece, and then a victim got up on the stand and she quoted the kind of care she got from the call center, and it was terrible, and so ChoicePoint really took a beating that day.

Learn from the marketplace. There's all sorts of lessons out there, so be very thoughtful and learn. It's what I like to call the 360-degree approach, not just legal compliance, but have a company policy, self-regulate, get involved in the industry, bake it into your public relations. Vendor compliance, employee education is probably your greatest weapon. Make sure that you care for each of the individuals if they have issues, and them make sure that all the customer needs are addressed. That's all I have.

[Applause]

Danny Harris: Thank you. Thank you, Sheila. It was nice to see that Sheila and I only disagreed on one thing. I would give up my Social Security number for a Dove bar.

[Laughter]

Yeah, I mean we're not talking Good Humor here. We're talking Dove bar. It was very touching to hear her open up her vest and share that she has both a coffee and alcohol problem –

[Laughter]

– and you know, that's where it starts. You have to at least recognize it, and that's where it all starts. So, we're praying you. But seriously, folks, thank you so much, Sheila. That was great. Richard, how much time do we have? Five minutes? Any quick questions, folks? Okay, there's one. Yes?

Audience: _____ constantly changing _____ do we get a handle on that? You know, what about data _____ how do I know where we stand?

Danny Harris: That's a very good question.

Sheila Colclasure: Again, at our company, at Acxiom, we deal with every bit of data that you could conceive of, and we have to have bright line rules around how to treat it. So, for a date of birth standalone, remember, PII is very contextual. If you have DOB, it's as sensitive as an SSN if it's tied to a name because there's not very many – there's actually nine Sheila Colclasures in the U.S., but there's not one of them born on my birth date. So, that combination gets you right to me, and it's the keys to unlock my bank account, et cetera. So, date of birth in combination with name, very sensitive and absolutely PII. A date of birth standalone, no sensitive at all. It's just a day and a year.

Danny Harris: And here's another tip that Sheila actually provided earlier in her presentation. As an organization, as a company, pay attention to the data you're collecting, and if you don't need to collect it, don't collect it. That's absolutely key. There was another question up – yes?

Audience: Someone mentioned at another session, they raised the question what happens, since we're working in aid offices and we frequently receive calls from the students or from their parents, how are we supposed to answer certain questions that may arise without really having some way to authenticate who the individual is, and then

not being perceived as not being helpful to the individuals who are calling in for assistance?

Danny Harris: That's a good question. I don't have an answer. Sheila?

Sheila Colclasure: I would ask what kind of call is it? Are they calling for general information or are they trying to get in the account?

Audience: They're calling for information about their financial aid.

Sheila Colclasure: Okay. Okay, so then you need –

Audience: For instance, "I want to know if I'm receiving Pell to cover my tuition –

Sheila Colclasure: – right.

Audience: – bill this semester."

Sheila Colclasure: You need to have an authentication process for your calls. You have to devise a plan, and there's all sorts of ways to do that, but you have to have authentication and you have to have training. Anybody who's gonna receive a call has to have the training. You have to implement a process.

Audience: Could you just give us an idea of what sort of authentication you could –

Sheila Colclasure: Well, I mean you could certainly ask the out-of-wallet. You know, I'm calling in, "I need to know about my student aid. Can you tell me?" "I need to authenticate you first. Can you tell me – " you know, have three questions that you ask, right? Or maybe four, and they can get one wrong but they have to get three right, and the questions are things that only the student would know and that are specifically in the file. Now, you don't give out the answer. We have a lot of clients that do this authentication. The financial services industry, which we serve a lot, we serve all industries but they are the most advanced in using technology. They collect the most data, and they also have the most technological advancement. They've just been investing in this space for years, right?

All of them have authentication when you call in on the phone. Either you have a PIN that you have to key in, or they say, "What's your security word? What's your identity code? What is your PIN? What is your mother's maiden?" They have a series of authentication questions when they're dealing with a live person, and if you're gonna be talking about confidential, private, sensitive information, you need to have an authentication procedure for the

phone, and you need to train for it. So, you need to devise it, document it, disseminate it, and hold it accountable.

Danny Harris: I think we have time for at least one more question, or two more. Yes?

Audience: In response to what she was saying, I know in my office I have my staff to ask the extra question. I always tell them that, "Always ask the extra question," and that way they're able to authenticate who is really calling and what the information is, because a couple of times we've tripped up some of our off-campus landlords who are wanting to find out about the students' refunds and when they're getting them, and all of that stuff, and I had one landlord say, "Well, I'm not really the parent. I'm just trying to find out when they're getting their money." So, we do that because – and sometimes they think it's frustrating to do, and we get some parents who get a little upset with us, but being here this week, I said, "New game, angry parent instead of angry _____, somebody ought to invent that," because we're just trying to protect people's information, and unfortunately, for those of you who are not in the financial aid world, who is the worst person who comes to us to try to get the information? It's the parent these days, and they are overbearing. They're overbearing. I have been cursed out more this year than I've ever been cursed, you know?

Sheila Colclasure: So, I would say handling an angry parent, have a methodology, a script that you give them, "I'm sorry. We're implementing a new authentication process to protect your child, the student. This is very important to the school, that we protect your student, your child, the child's information. I need to authenticate you." So, devise a script in advance that you read, and equip them with that, as well. I mean what you talked about, that's a great example of social engineering, and it's the most effective way to get at private, sensitive data, because we're all emotional human creatures and we respond to other emotional human needs. It's in all of us to try to be helpful and nice, especially if you're in the service industry, so getting tricked like that is pretty typical, and so I think devising a script, disseminating the script and the plan, and equipping them with the right things to say to diffuse angry parents is an important thing that you guys should probably implement.

Danny Harris: Fred, you have the final question.

Audience: Yeah, just one general one. I guess the financial aid offices are just one department in the post-secondary community. I was curious if the financial aid offices are getting any general guidance from the CIO governance structure from the broader university

community, and how we can converge that with what we're trying to do.

Danny Harris: And I'm not sure about whether it's occurring at the university later, but I believe it is. But certainly, what we're trying to push down, and we talked about it earlier, is the awareness program and the fact that the awareness program has to be holistic and it has to be across the entire enterprise. So, I think the answer is yes. Folks, thank you very much. Appreciate it.

[Applause]