0:00 slide 1	Hi everyone, this is Kimberly Madia here, I'm part of the InfoSphere product marketing team. And today I'm going to talk to you about securing and protecting your data across the enterprise.
0:12 slide 2	So on slide 2, we have an agenda. The first thing we'll talk about is Information Governance, we'll define what that means. Next we'll talk about protecting sensitive data and some challenges around protecting that sensitive data. We'll talk about what are some risks and what's at stake, if you do not protect that data. Next we'll take you through an approach to ensure that you have a holistic data security and privacy strategy in place, and there's three aspects of this approach : understand and define, secure and protect, monitor and audit. We'll take you through each of those 3 categories and give you some hints and tips for setting up your security and privacy strategy, and finally we'll go through some client success stories for some folks who are using our InfoSphere Solutions for Information Governance today.
1:06 slide 3	So if we move to slide 3, I just wanted to set the stage and talk a little bit about what's happening in the world today. As you know the volume of information is really exploding. It's very mind boggling. Organizations today are collecting information from many many sources. You know we have the traditional formats, whether it's a web application or voice input. But we also have some new sources of information such as GPS systems, RFID tags, streaming videos, real-time data, and making sense of all this information and making it valuable to your business is really important. It presents a challenge but it also presents a real opportunity. If we can bring this information together, if we can orchestrate the people, processes and technology around this information, we can really achieve a better business outcome. And we can manage our cost better and we can achieve a better business result. But this really lays the foundation for an information governance strategy. With this explosion of information we have this opportunity to become more intelligent as corporations, but we have to establish a framework for driving that intelligence. That's where information governance comes in. It's going to help you streamline your business processes, it's going to make sure that

	you're compliant to policies, laws and regulations, and it's going to help you control cost and optimize your infrastructure. You're setting up an information governance approach, we'll really help you manage this volume of data that's coming at your company today. And it will bring together your people and your technology to produce a valuable business outcome. So what we are going to talk about throughout the rest of the presentation is a little bit more on what information Governance is, and then specifically how security and privacy fit into that big picture.
3:12 slide 4	Then I'm going to move to slide 4. So what we have here on slide 4 is a picture of what information governance means. When we talk about information governance we really need to think about the full lifecycle of data as it comes into our enterprise all the way through from when it's retired, archived and removed completely. And throughout each phase of the data lifecycle we really need to be paying attention to the governance of that data. We need to make sure that it's of high quality, that it's secure and protected, that we are being compliant with the data as it exist throughout it's lifecycle. And some of the major phases of the lifecycle we have highlighted on this slide, first stage is kind of managing that data, what we mean by that is making sure our data is stored properly, it's in the database, it's in a content management system, we understand how it's stored and kept, and then the next phase is this integrate based, and this means bringing together different sources of data to derive value. And this could be in technologies like Master Data Management or Data Warehousing. And then finally the analysis phase where we are really going to be doing some analytics and trying to derive some intelligence from our information. So throughout each of these phases, throughout manage, throughout integrate and throughout analyze, we want to make sure that we are governing our information and Governance covers all of these 3 areas. And the key components of governance are quality, lifecycle, security and privacy and standard. And what we are going to talk about today is security and privacy.

	We will talk about what are some strategies for security and privacy and what you need to do to develop a holistic approach to security and privacy rather than a peace meal approach and how you can ensure security and privacy across each of these 3 phases of the data lifecycle. We want to make sure that that data is secure and protected and during the manage phase, during the integrate phase and also during the analysis phase. So go through a complete strategy offer that.
5:22 slide 5	But first, on slide 5, we wanted to give you a little bit of background about what's motivating the focus around security and privacy. And really, it's this worldwide attention we have to protecting a private and sensitive information. And you'll see on this slide, regulatory bodies are coming up around the world, that govern the use of private information, it's not just something that's happening in the United States or in Europe, all over the world governments are focusing and requiring organizations to protect sensitive data. Really all over the world, and something else to keep in mind too is, if you are a global company doing business with customers or you have partnerships around the globe, you are required to be compliant with those laws and regulations as well. It's really important that you have an understanding of these laws and figure out which ones are going to more important to your business. This is really the number one driver, this is why we are so concerned and so focused because no one wants to end up facing fines or jail time or other negative consequences because they are not in compliance with these worldwide mandates.
6:37 slide 6	So on slide 6, I wanted to share some interesting data too from one of our top analyst from Forrester Research. They recently did a study that was published in February 2011, regarding priorities for IT organizations. And you'll see, 90% of those surveyed said data security was a top priority for them in the next twelve months. So organizations are really feeling this push, these laws that are being enacted around the world are becoming more and more urgent for organizations. And another big thing almost 85% of people ranking this as a high priority, is managing vulnerability and complex risks. The world is really becoming more interconnected, there's a lot more

	threats and vulnerability points out there, this is really of top concern for organizations so, we at IBM, want to help you with these top 2 concerns, and give you some assurance there is a way to protect your data while also ensuring that you're compliant to these worldwide regulations.
7:44 slide 7	So next on slide 7, what's at risk? One of the question I get often is : hey, I hear there is a lot of regulatory actions going on but I'm not convinced that I really need to do it, you know maybe it's a little bit over hype, maybe governments are going too far, we are being over regulated. And I would say that is definitely not true. The risks, as we can see here on slide 7, are very real and the threat seems to be increasing pretty much daily. This is becoming a very very hot topic in the news around the world. I wanted to kind of share a couple of example on this slide about some real world examples that have happened to companies with a global presence. One you may have heard of we have on the slide is the example of the Sony breach. There were some malicious hackers who compromised Sony Playstation and they stole names, addresses, countries, email, birth dates, passwords for Playstation, logins of 70 million Playstation users around the world. And these hackers wanted that information and they also wanted to show Sony that they could do it. It becomes more of an ego thing for the hackers. They just want to prove that they have the knowhow to go in and compromise a big company like Sony. Certainly no ones want to have their personal information hacked into especially passwords or handles they might use to play the game. That's one of the examples that really affected users worldwide. Another example is an SQL injection threat, know as Lizamoon. So what happened here was, 28 thousand websites were infected with malicious code because of this SQL injection attack and so what happened is this malicious code was being infected on different websites and going into various databases and extracting sensitive information from their databases. So SQL injection threats are very very real. Lizamoon is the largest and fastest growing in history and it already infected 28 thousand websites and that number is growing by the day.

	Another good example is something that happened actually with US government institute, the FAA. They were using a third party for their application development and testing and that third party compromised records of 45 thousand employees. This is very personal data on US citizens, it was all compromised because the government wasn't using secure testing practices. Something that is often overlooked is, these non productive environments. We tend to have more strict controls on the databases and applications that we use for our production, but you don't forget to think holistically across your enterprise and think about non-production environments, these are also very vulnerable. And the final example I'll talk about here was the WikiLeaks incident, regarding US wars in Iraq and Afghanistan. A private in the US military got access to information that he shouldn't have, he passed it to a journalist and put the US national security at risk. As well as individuals who were named in this report. So these are some examples from various different industries affecting government, affecting people, affecting our faith in using the internet. The risks are very real, these are very recent examples, and it's not just rules and regulations it is also very real risks and these very real threats that are driving the need to think about security and privacy.
11:39 slide 8	On slide 8 I wanted to take a step back and say ok where do we go from here? What are my choices? We all agree that the volume of information is growing, there's a lot of sophisticated hackers out there, there is a lot of vulnerability, so what can we do about it? Well one, well we could just do nothing, bearing in mind that there is a lot of regulation happening out there, the body of regulation and the volume of information seems to be growing by the day. The requirements for security and privacy are becoming extremely complex, especially with the proliferation of mobile devices and various end points. And I also found some interesting research here, 73% of security professionals say the volume of database security attacks will increase. The average cost of a data breach is going up. This year the average cost in 2.7 million US dollars and 95% of

	compromised records originated in database servers. If you are comfortable with these numbers, you're comfortable with these risks, then you can probably do nothing. But I don't think any of us would feel very comfortable putting our companies and our data open to this kind of risk. So we probably need a better approach here. So do nothing is probably not the best way to go. Another thing we could do is maybe leverage some of the solutions we have today. However I would caution you that usually when we have manual or home grown approaches, they meet a higher risk, they are not very efficient and they may not scale as that volume of information grows. And also, homegrown solutions may not be poised to handle new kinds of threats, new kinds of hackers, new kinds of vulnerabilities. The malicious users out there, their talent, their complexity, their ability to penetrate environments is really increasing. We can't necessarily rely on our home grown solutions to keep up with that sophisticated hacker mentality out there. We would not recommend that you focus on your home grown solutions, rather we would suggest implementing a holistic data protection strategy. And for the rest of the presentation we will walk you through what we mean by that and give you some hints and tips on how to get started. What is unique about our recommendation here, it's not another process heavy approach that you are going to take, this is something that you can simply implement into daily practices, into your daily best practices, to improve data security and privacy. We don't want this to be another initiative that gets ignored or something that is so process intensive that it is really meaningless and not providing you any value. That's really the goal here, it's to help you with every step of the way, include data security and privacy into the best practices that you do today.
14:31 slide 9	So on slide 9, I've highlighted some key questions that get the juices flowing and things you might want to think about as you look at your data security and privacy approach. One good thing to think about is where does your sensitive data reside across the enterprise? Think about the complex environment you have, think about

	business partners that you work with, think about production and non-production environments, you'll really think holistically here. Also think about the outsiders and insider threat. We focused a little bit on the negative consequences of attackers, malicious outsiders coming in, but what about your internal users? We don't like to think about our internal folks as being malicious and evil but they could make a mistake or do something inadvertently that could compromise protection and security and privacy. And also think about how you're sharing documents across your enterprise, who is seeing information as it is being passed from the different roles within your organization and what kind of information is being shared externally with third parties, whether it's a customer or a business partner. And then finally, think a little bit about your databases, how can you protect those, monitor those, lock those down, would you be ready for an audit? Could you produce an extensive audit trail about who and what was coming into your database and when? Those are often required by regulatory compliance mandate, so you really think about these databases, they are a big source for attacks. And also you want to point out the quote here: we are moving away from security and privacy as just an IT issue. Really this is a business concern, it's not something that is just the worry of the DBA. The data really is the lifeblood of the business and we are seeing a shift and a focus in the C-suite on this problem, and that's really good because to do this holistic approach correctly, it would have to be a team sport, and everybody has to be on board so our work will kind of encouraged in this shift and I just wanted to point that out, and hopefully in your organization, whether you're and IT or a business, you're having that interlock across the organization so that you can achieve the best possible strategy.
16:45 slide 10	Next on slide 10, I wanted to take you through what's IBM's approach is. We bring to the table a wealth of experiences, we can provide hardware, software and services for you, to really build a strong foundation for your strategy. And we have been focusing on for this

	presentation is data and information, but also wanted to make you aware that we can also help you with identity management, application security, network security and end point security and physical infrastructure. We have a whole foundation in place. What makes us unique is we are not just here to provide you with the technology, we are here to help you implement a holistic process and give you best practice and expertise rather than just throwing another piece of software or hardware at a problem. So I just wanted to point that out, and for the rest of the presentation again, we are just focusing on the data end of information but we have other areas as well to help you.
17:39 slide 11	So what is our approach to data and information security and privacy? As you'll see here, on slide 11, we have a 3 tiered approach. The first tier in understand and define. You really can't protect information if you don't know where it exists or even if it exists. We have an interesting exercise we take our customers through, we ask them to identify enterprise applications and databases and they usually have some idea what their major data sources are and applications, but we have a tool that can actually go through and automatically discover data sources for you and applications, and inevitably there is a disparity between what we think we have and what actually we have in reality. You're opening yourself up to some big risk if you don't even know that the data source exists. And understanding and defining also incorporate understanding relationships between those data sources, how often that data is accessed, what types of data you have, and also you're trying to figure out some policies and definitions for various data types. As new data comes in, it should be categorized into a correct category, and privacy and security policies should be set up based on that particular category or definition. That way you can be assured as that data moves through the lifecycle, that the appropriate controls are put in place. So understanding and defining is really a very first step you always should take to see and understand what you have and if new data comes in, you have a process in place for defining it and for setting up policies to ensure security and privacy. And also part of that is having a matrix in a standard approach so that you can demonstrate and prove that

	that piece of data is protected and secure. The next pillar is secure and protect. Secure and protect is really the implementation of those rules and policies and procedures that you've identified in the first phase. And here, we bring in many different technologies depending on your organization and depending on what your needs are. We can do things like data masking, data redaction, data activity monitoring, test data management, a bunch of technologies here as defined in the first column. And then finally we have monitor and audit. What's unique here is, it's not enough to just define your policies and implement them, you have to be able to demonstrate and prove to a third party that you are actually compliant and that you are protecting that sensitive information. And this is a step that is often forgotten and we want to really emphasize it here as a very key and critical step. Because, it does no good if you can prove it to a third party auditor that you are protecting and securing that information. Also part of this monitor and audit is the idea about continually assessing vulnerability over time. You may have locked down and protected the data against a particular threat, but if a new attack comes or a new source of threat arise, you need to be able to ensure that you are going to be protected long term. So these are the 3 areas to think about as you are developing your holistic approach to security and privacy, and what we'll do for the rest of the presentation is go to each pillar and talk a little bit more detail about what they mean and some technologies that we have available to help you.
21:12 slide 12	So on slide 12, as we mentioned before, you can't protect information if you don't know it exists and you don't understand it. Often companies have a very distributed data landscape, and corporate memory is very poor, we don't necessarily have everything documented about why created a database instance. We need to be able to get a clear crisp view of this complex enterprise, we need to keep in mind the data is distributed over many different applications, platforms and databases, we really need to get a handle on this as a first step in understanding and defining what our

	protection policies will be.
21:54 slide 13	And then on slide 13, something to keep in mind too is, we need to remember that data is related, and that we need to understand those relationships, because if we protect only one piece of it, we may be vulnerable in another area. We really want to mention here is, we want to make sure that you understand those relationships as well because, they can uncover and lead to other data that can be sensitive that we didn't notice at first. Also as part of this understand and define area, we want to take the opportunity to finally document our data sources, our applications, those relationships so we don't have the same problem again of not understanding what our landscape looks like.
22:36 slide 14	So on slide 14, I just wanted to give you an example of what I mean by this so you can see very concretely. As we mentioned, sensitive data can't be just found by just doing an initial data scan, you need to look a little more deeply and figure out how the relationships exists. In this example, how would you know that a patient ID is imbedded in a number within another table. It really would not be possible to find that information if you didn't have some kind of automated approach to finding this hidden relationship. So here you can see the example, we have table 1, where we have the number of John Smith, and then we can see in table 15, that patient number is related to a particular test and that test actually can be revealed in another table to be a specific diagnosis. So if you don't have a system that's looking for this complex relationship, you could easily find out what John Smith's diagnosis is. And that's exactly what we want to avoid, that the kind of complexity that exists out there, we want to ensure that you are protected. Automating the discovery process, having a good data discovery solution where you can find these hidden relationships is really going to be critical or you won't be able to develop that holistic protection approach that we feel is important.
23:58 slide 15	So the next area I wanted to go into is on slide 15, and this is the secure and protect area. As we mentioned a little earlier, you have to remember that you need to protect against those internal users as well. We know the hackers threat is out there but making sure that your "power users" know that they are being watched every minute is really important.

	Another thing to think about in this secure and protect area is: what about misuse of those with proper privileges? So for example, if I'm a physician I may have very legitimate access to a patient medical records, but I don't want to abuse my privilege and just look at the medical record because I'm curious or because I'm interested. I only want to be able to look at this medical record if I'm actively treating a patient. So making sure that even if you have the right privilege, you're not abusing these privileges, is a part of secure and protect story. And also, other things to think about here in this area, how do you prevent risk from happening if someone walks off with the backup tape, or there is data on a physical media like a Sun drive, or a laptop get stolen, how can you be protected there? The secure and protect area is very broad and there is a lot of subtleties and complexities here so we really wanted to remind you to think about all of these different things. And think about someone walking out with a back-up tape, think about any third party who might come in contact with your data, think about monitoring those "power users", ensuring that people who have daily access to the data aren't also the ones responsible for setting the security and policies. You want to make sure that they are separate and distinct so you don't have a conflict of interest there. Lots of subtleties here but all things that are very very important to think about when you're developing your strategy.
25:52 slide 16	So on slide 16, what is that holistic 360 degree strategy that we recommend for securing and protecting your data? First we want to say, think holistically across your environment, across production and non-production environments, and think about what type of data lives there. You have your structured data, which is that data found in databases such as Oracle and DB2, Informix, Sybase, Netezza. Also think about your unstructured data, that would be data not in databases, like in file shares or documents or scanned images. Think about online data, that data that is used in everyday use, and

	then offline data, for example data kept on a backup tape or some drive. Think about all these different types of data, think about where it lives across your enterprise. And then we have various technologies that we recommend, for login in and protecting that database on its data type. For example, for structured data, we recommend things like data encryption, data masking, database vulnerability assessment and database activity monitoring. For unstructured data, we recommend things like data redaction and monitoring to file shares and monitoring access into the cloud. And then online data again, database activity monitoring, data masking comes in here, as does data encryption. And then for offline data we recommend encryption and also data masking. As you are trying to address all those diverse threats that we outlined in the previous slides, again there are threats coming from the inside, those coming from the outside, from malicious hackers, those inadvertent things that might happen for example, like a lost backup tape. You really want to think about all these different types of data we have. You really want to think about the set we mentioned earlier, you really want to think about this holistic approach that we recommend, think about the type of data your trying to protect and we recommend these different technologies to best login and secure that data.
28:09 slide 17	So what we would like to do next on slide 17 is go through each of these data types and the technologies that we recommend, just to give a little bit more inside information on what those technologies do and how they protect the data. So we'll start with the unstructured data type. To protect unstructured data, we recommend a process called redaction, and what redaction simply is the act or process of editing or reviving a document so that the sensitive data is completely removed. Very simple, very basic, and you can see in an example here on the right hand side where we just blacked out that sensitive data.

	We can also, if you don't like the black marker approach you can insert some meaningful text, for example, if you remove or redact an account number you could simply insert a string that says account number and that data would be hidden and protected. And what is interesting about redaction is it's not a replacement for other types of technology. We really want to use redaction as part of your holistic strategy, it's not encryption, it's not a substitute for access control, it should really be part of a secure document lifecycle process. And again it's just taking that unstructured data that you have out there, that data and scanned files, and image files and word files, and removing sensitive information, so that document can be shared and passed among different parties internally and also externally. When you think about unstructured data, you remember redaction, that's just a way to remove that sensitive data from the documents, to black it out so that unstructured document can be shared internally and also externally. So, one of the things that we recommend when you are evaluating a redaction solution, is to ensure that it is fully automated.
30:05 slide 18	So on slide 18, we kind of talk about what we mean by that and why it is important. We think about all the unstructured documents that you have in your enterprise, they likely live in an enterprise content management system. And there are thousands and thousands of documents, and it is very tedious and time consuming do to data redaction, document by document, line by line. So when you are considering an approach to redaction, make sure that it can do a batch processing, be very automated, that's really important. Also ensure that it supports diverse data formats, so you likely have PDFs, text files, tiff files, Microsoft Word documents, a bunch of different types of documents. You have to make sure that a redaction solution can handle all this different diverse data types and also ensure that it can protect that sensitive data types found within those documents. Just a couple of notes of caution, there is a lot of different redaction solutions out there, when you're

	looking for one, look for one that is automated and that supports a very robust data type, because you probably have many many different types of documents out there.
31:12 slide 19	So next on slide 19, I wanted to move to the structured data values, so redaction for unstructured data and for structured data, we recommend data masking. And what data masking is, it's a process or a method for creating structurally similar but fictional information. And the purpose here is to protect the actual customer data or the actual sensitive data that you have, while substituting a fictitious value so that you can facilitate processes like good testing, good QA, good development. So a developer or a QA analyst doesn't need to test on real live sensitive information. A substitute that is contextually accurate will work just fine. So with masking, we give you the ability to add data that have the same look and feel as real live data but it is not actually customer sensitive information. And other terms used for masking are things like obfuscation, scrambling, data de-identification. And that's what we recommend for your structured data values. Those data values that are living in databases, we recommend that you use data masking, and what is really nice about this, is that it allows testers and QA people, you may have a disaster recovery team, it facilitates their job function, they can get their job done, but they aren't exposed to any sort of sensitive information. What we have been talking about is static masking, and this is a way of extracting rows from databases, masking the values and then putting them into a new database for testing, or QA, or disaster recovery work, or training. But there is a new area emerging in masking called Dynamic masking, and what this means is it masks data on the fly, in other words it doesn't take the masked values and put into a new database, instead it's just returned to the user, so the user doesn't know what's masked and what wasn't masked. So this is a up and coming area to watch out for is Dynamic masking, this term was coined by Gartner. But what we are talking about here today is really static masking and again that is for protecting that structured information in

	non-productive environments.
33:34 slide 20	Moving to slide 20. Why is this important to think about? Why is protecting information in non-production environments often overlooked? Really is it because so much attention is focused on production environments and that is where all the security is in place, the worrying about non-productive environments is kind of atrophied and we don’t have time to do that, and it’s seems like a secondary thought. We can do when we trust our business partners, our employees more than we trust external users but this database still has the same level of vulnerability and we are still required by law to protect it. So unfortunately what many company do is, they just clone their production database one for one and row for row, so you essentially have two production copies and that test database is then shipped off to partners or other divisions to handle the testing. And while this is very simple and easy to do, it doesn’t require a lot of knowledge or the understanding of the subtleties of the database, it does cause problems for security and privacy. So that's really what we are drawing out here on slide 20 is that, it’s not very secure and also it takes up additional space that we don’t really necessarily want to spend money on. For example, we essentially have two full sized production databases and our testers might only need to test on small subset of that data. So it doesn’t really make sense to maintain these two whole copies.
35:11 slide 21	So on slide 21, we recommend what a better approach is. And what we recommend is creating this masked version of your production database. That way you can take a smaller sub-set of your production environment, secure and protect the data in it and then use it for whatever purpose you may need, whether it’s for testing or training or development. This masked database is fully secure, fully protected, no risks associated here, and you can also manage your storage cost a little better because you only need to take a small sub-set of production to ensure that the testers, training teams and development teams have what they need. A lot of advantages to doing smarter secure testing. And that’s what we wanted to draw on slide 21.
35:58 slide 22	And on slide 22, I just wanted to give you an example of another way you can do testing. If you don’t want to do a sub-set of your production database, and have all of

	your developers and testers access that sub-set, you can instead do what we have pictures here on slide 22, and just have each of the teams a point of sub-set from production databases, so sub-setting and masking and masking into each of these different environments. It depends on the needs in your enterprise, how you want to handle it. But these are both better ways than just cloning your production environment for testing. Here as you can see, we take a small sub-set of the data from our production environment and let the testing teams and the training teams and the development teams deal with that sub-set in that secure masked sub-set. So just food for thought here, think about those non-productive environments, think about doing a sub-setting so you don't have to maintain full size production clones and think about all the other users who may need access and make sure that it's masked and protected so that you have minimal risk.
37:08 slide 23	Ok moving next to slide 23. We've covered the structured and unstructured data and some technologies to protect them. Next we are going to move to online and offline data. And what we recommend here is we recommend encryption. What is good about encryption is that it transforms data to make it unreadable to any malicious person. The only way the data can be readable is that if you have a proper key and you have the proper rights to view that information. The original data is preserved in full, so that is why we recommend this for production environments. You can see an example here. If someone were to intercept an encrypted data, they would see just a bunch of garbled mess, totally meaningless, doesn't make any sense. But if they have the right key to decrypt they can extract and get back the original data that was encrypted. So, I recommend this for online and offline environments and definitely a great way to ensure that your data is protected and locked in.
38:14 slide 24	So on slide 24. There is a lot of approaches to encryption out there, I'm sure you can name a few of them. So I wanted to give you some advice on which encryption strategies work. We recommend a file level encryption. This is because it tends to be the lowest cost and provide the highest value. It promotes separation of duties so you don't have your DBAs also managing the encryption keys, you can keep them

	separate and distinct. It allows you to proceed with protection without having to change your underlying infrastructure. So if you employ a file level encryption approach, you don't have to do application rewriting, you don't have to change your database scheme. You can just insert this above the file system level, insert a key management approach and you set up a security administrator to set up and define the keys and to manage the key management process. You don't need to worry about having a DBA be responsible for this or asking any of your application people to make changes to the application or rewriting. So your file level encryption is a very scalable way to protect your data without having to do any kind of application changes since it goes right in the file system level, you don't have to worry as your databases grow over time, that your strategy will also scale, this is what it is about encryption. So what we have covered so far in the secure protect area, that we want you to take away from is, you really need a holistic approach to security and privacy, you need to think across your complex heterogeneous environment. Think about the type of data that exists, we have unstructured data, we have structured data, we have online data and we have offline data. We have different technologies that we recommend to ensure that you are protecting each of those data types. A quick rule of thumb, when you think about unstructured data, think about redaction. When you think about structured data, think about data masking. When you think about online or offline data, we recommend file level encryption. So that's just a way to get you started in some specific technology you might want to look at as your looking across your very complex environment and all the different type of data that you may have.
40:26 slide 25	So what I'd like to do now is move to slide 25 and talk a little bit about the monitoring and auditing. As we mentioned earlier, you need to be able to prove to a third party that you are compliant. And to avoid fines, to avoid other negative consequences like jail time, you need do be able to prove to an auditor that you are compliant. And you don't wait until it's too late, you don't wait till you have a data breach, you think about having a process in place so that you can demonstrate

	compliance to auditors. It's really important to close the loop on that process, you might have all the good protection implemented in place but if you can't prove it, it's not going to do you any good. Keep that in mind as you roll out your security and privacy approach.
41:13 slide 26	So slide 26, some things to think about around the auditing area is, you want your auditors to come in and have a very simplified process, they should be able to be empowered, they shouldn't need to be talking to any folks from IT or the business. They should be able to pull the reports that they need on a variety of different activities, including users activity, object creation, database configuration, entitlements, they should be able to be empowered and do this for themselves. They should be able to see a clear separation of duties across your enterprise, they should be able to trace what's happening across your applications and your databases, and they should be able to sign off, escalate processes automatically. So you look for a solution that provide these capabilities to you. If the auditor comes in and has a very easy process to follow, they are going to feel more confident, they are going to feel like you have your act together. So ensure that they have that ability. And you do some things to keep in mind you're king of evaluating what would be a good solution in this area.
42:19 slide 27	So on slide 27, I just wanted to show you an example. This is from our Infosphere Guardium offering, and you can see an example of these automated kind of reports I was talking about. What we do with InfoSphere Guardium is we give you the ability to generate these auto-report files automatically and an auditor can escalate or write comments, or create an exception. And everything is very documented, straightforward and very visible. And we think thatit sets up apart as an offering here because of the simplicity because of this control that we can give the auditors, it really makes them feel empowered and they can get the information they need without having to bother the DBA or a business person. And that makes sense too, because a DBA and a business person in your company, their job is not to satisfy the auditors, they have a goal, they don't want to be distracted in their daily work. So let the auditors come in, let them handle this and let your IT specialist and your business analyst focus on their day jobs.
43:17	So on 28, I wanted to provide you with information

slide 28	about what IBM offers. We really covered a lot of different areas around security and privacy, we have given you an idea about these three pillars to focus on. So i wanted to let you know what the InfoSphere offerings are in this area and what the strength are and differentiation are. First we have a product called InfoSphere Discovery that does that automatic detection of sensitive data that we discussed, we have a data masking offering called InfoSphere Optim Data Masking. We have a solution that does auditing and database activity monitoring called Infosphere Guardium. We have an encryption offering, Guardium Encryption and then finally we have Guardium Data Redaction which does the redaction that we talked about earlier. So I wanted to let you know that we have solutions available across all these different pin points that we discussed and really encourage you to think about what is your most pressing need in your organization, we understand you don't want to adopt all these different technologies or all these different approaches, but the way our solutions are designed, you can start anywhere and build. So if you have a particular paying point around encryption, you can start there and be assured that when you're investing in IBM, you're investing in a holistic framework. Our solutions are scalable, modular, they fit together nicely. So you can be assured as a new problem comes up or you want to tackle a new threat, our technology will be integrated and marked together going forward. The end goal here is to satisfy compliance, ensure that you are going to be ready for those audits and protect sensitive data whether it's customer data or some trade secrets that you might have.
45:01 slide 29	Ok moving to the next slide. So what I wanted to do for the rest of the presentation is just to walk you through some client's examples real quick. These are not new technologies, they are in the field used by many many, huge corporations around the world, so they are time tested and true. So we really want to make sure that you feel comfortable with that. My first case study here is from a leading global household goods manufacturer based in the US. And

	they had a need to protect HR information in non-production environments. So they used our InfoSphere Optim data masking solution for SAP applications, it enabled them to be compliant, it enabled them to protect sensitive data in non-productive environments, it helped them speed up their testing cycles as well, and also we were able to deploy this in much much quicker time than if they would have developed their home grown masking solution. The real benefit here is they were able to save time, they we able to improve their testing results and they were able to ensure compliance to privacy regulations. So your really good story, a big SAP customer of ours, protecting HR information in non-production environments.
46:23 slide 30	So the next slide, on slide 30 is another example of a customer really struggling with meeting compliance regulation. In this case it was PCI DSS. This customer is actually based out of the UK, they are a health care provider and one of the cornerstone of their business was their ability to protect their customer. As a health care provider, their brand recognition was built on privacy, ensuring privacy and making sure that sensitive medical information was kept safe. And their customers felt empowered and appreciated and they really wanted to make sure that their good brand name was maintained while they were dealing with PCI DSS requirements. So they employed the Guardium Data Redaction solution because they had lots and lots of medical records that they needed to share across the organization and with the customers they needed to protect the sensitive data in those documents. And one of the benefits they found using our data redaction solution, is that it was very very accurate, they could set up the batch process, that they were redacting documents quickly and on the fly and they were able to satisfy compliance requirements in a very kindly matter. If they had to do this themselves they were looking at months and months. And with us, they cut that to just a few weeks.
47:44 slide 31	Ok moving to the next slide. Our next example is one that we have for encryption, it’s an example here of a financial software provider. Before we go into the details of this use case, one thing I wanted to mention is you’ll see all these clients examples and successes

	come from many different industries. We have health care, we have a manufacturer, we have a financial software provider. So these regulations are really affecting many many different industries. So I just wanted to point that out, that no one is really immune out there and these laws are really touching many different industries. So what we have here was a software provider, again as a financial provider they had lots and lots of credit cards information in their enterprise, so they really had to deal a lot with PCI DSS. By using Encryption Expert they were able to set their privacy policies once, they didn't have to go to every single database across the enterprise and define the policies. They could do it once and ensure that their policies would be deployed throughout the enterprise. That was a real advantage there. They could keep up with the high level of transactions that they were seeing and they could ensure that they were protected. Because they could just set a simple policy once they have it be deployed quickly throughout the enterprise.
49:02 slide 32	Moving to the next slide. Our very last customer example. This is from a leading technology company. They had to deal with SOX and PCI, and they had a very very large environment. What they wanted to do was really make sure they understood what was happening in their databases. They had 725 databases across their organization, across 10 data centers and they had a very aggressive time schedule for figuring out what was happening at the database level, what requests were coming in, who was making those requests. And we were able to help them with our Guardium Database Activity monitoring solution. With Guardium, they were able to implement a non-invasive with minimal performance impact. They could see what was happening at the database and really provide auditors with a good report of what was coming in, who was asking for the data, how often, made it very easy for the auditors, give them that transparency that was required in the compliance regulation. So finally I just wanted to end on why should IBM be your trusted partner here. One, we have many many thousands of professionals

	working around the world to understand each of these compliance regulations in, to be able to recommend to you appropriate technologies. We also manage security solutions for 400 thousand IBM employees, so we are a big company and we use all this good technology internally as well. And again, we’re able to tailor our solutions to meet your needs and with the InfoSphere offerings who are scalable and modular so you can pick and choose what you want to focus on. and know that you are buying into a process and a methodology, not just another technology. Our goal here is to enable you to have security by design, and not just throw another product at the problem, but rather implement best practices and augment that to the processes that you are using today. To really make sure you’re secure and protected. Thank you very much for taking some time to listen and appreciate it. Again Kimberly Madia here, from the InfoSphere group, thanks for your time today.