RECORD, Volume 26, No. 2*

San Diego Spring Meeting
June 22–23, 2000

Session 78PD
E-Commerce Series: Risk Management for the Internet

Track: Nontraditional Marketing

Moderator: JAY M. JAFFE
Panelists: JAY M. JAFFE
STEVEN TIPPINS†
DAVID WESLEY‡
Recorder: JAY M. JAFFE

Summary: A discussion of risk management issues for e-commerce insurance products. At the conclusion of the session, the audience should have an increased knowledge of basic risk management skills and methods required for e-commerce insurance programs, as well as a better understanding of risk management for non-e-commerce insurance programs.

This session is valuable to persons with or without prior knowledge of risk management concepts.

Mr. Jay M. Jaffe: The presentation is, in a sense, a wrap-up to the four other presentations you've had from the e-commerce track. Our session will discuss risk management for e-commerce programs.

I'm going to make a short introductory presentation, which will then be followed by presentations from Steven Tippins and David Wesley.

What is risk management? It is actually knowing all those things that you didn't want to know, or didn't have to know before e-commerce. However, each of the other two speakers will also give his perspective on what risk management is, so you might come away with three different definitions of risk management, but I think they'll be quite similar.

Why are we dealing with e-commerce? The first reason is it's expected in today's world. The second reason is e-commerce can be a low unit cost operation. The third reason is it is the only marketing channel that can actually turn out to be a zero

† Mr. Tippins, not a member of the sponsoring organizations, is Professor of Risk Management and Insurance at Roosevelt University in Schaumburg, IL.

‡ Mr. Wesley, not a member of the sponsoring organizations, is Vice President & Chief Medical Director at General & Cologne Life Re in Stamford, CT.

marginal cost distribution opportunity. Once you have your Web site running, the cost of the next sale is going to come to you at zero.
There are seven key factors I've identified for the long-term success in the e-commerce environment:

- brand recognition
- interaction with the right people
- instant order fulfillment
- low-priced products
- cost-effective marketing
- a user-friendly Web site
- a value-added Web site

Why brand recognition? Obviously buyers will react more favorably to the known than the unknown.

Web interaction with the right people is needed because not all Web users are potential insurance buyers. My friend Gary always says to sell, a company has to be in the right place, with the right product, at the right time.

Product delivery has to be instant. We know Web browsers are impatient. Traditional underwriting won't work in an e-commerce environment.

Low price might be the easiest of the seven factors to understand. On the Web there is either perfect or near perfect competition. Cost will become a primary factor for Web products, unless there is another differentiating factor.

Cost-effective marketing must exist if a company wants low-priced products.

If you want to have low cost, you'd better have effective marketing. Low price requires low cost.

A user-friendly Web site is imperative because not everybody is a techie. Remember a confused customer is a lost customer or, at least, a customer who won't return to the Web site for a long time.

Finally, to get people to return to a Web site will require something special. Having a value-added Web site will help to maximize the return of customers.

Risk management is important to e-commerce for three reasons: insurance companies don't like surprises, reinsurance companies don't like surprises, and insureds don't like surprises. I probably could add that insurance commissioners don't like surprises. The point is nobody likes surprises and a good risk management program will go a long way to avoid surprises.

One way to avoid e-commerce problems is to adopt a proactive risk management program. Risk management needs to be recognized as integral activity for e-commerce. You're going to have to figure out whether the product is going to sell, what the opportunities are for it, monitor the sales, and so on and then

monitoring the results. You can't start doing this five years into the program but you need to be prepared to do it immediately.
I attended a meeting for the chief actuaries in Sarasota Florida just a few weeks ago, and one of the presenters came up with his company's list of risk management areas:

- Asset risk relating to returns
- Asset liquidity risks
- Inadequate pricing
- Regulatory risks
- Reputation risks
- Operational risks
- Strategic risks

I also feel that marketing risks or lack of sufficient sales are extremely important since a company needs to start by covering the costs of product development.

It then follows that the next risk to consider is persistency. High lapses are going to lead to a problem with expense recoverability as well as morbidity or mortality antiselection. On the other hand, low lapses can generate an unexpected volume of claims.

Another way to look at some of these issues is whether a company should buy or build a new product. In today's world, you have these choices. Both can be viable options. The point at which a company wants to enter the marketplace and how much of the development costs it is willing to assume will affect its decision.

A good risk management program will look for early warning signs. Higher than expected lapses or a concentration of claims could be signs of trouble with an e-commerce risk management program.

Jumping on the Internet bandwagon is a serious commitment. It's now fashionable, but will it be the distribution answer? I don't think it's a marketing panacea. The Internet might not be a cheap or effective distribution channel. Just ask a lot of the companies that are selling products other than insurance.

The bottom-line is learn to be a risk manager rather than one that avoids risk. You don't want to take unnecessary risks, but you need to know how to manage risks. In the broadest sense, actuaries are good risk managers and keep in mind that the goal of risk management is to know all those things you didn't want to know or didn't have to know before e-commerce.

Our first guest is Steve Tippens. He's a Ph.D. and a faculty member at Roosevelt University where he's heading up a new insurance risk management program. Roosevelt University is in Schaumburg, Illinois, which should be familiar to all of us since it is the same town in which the Society of Actuaries is located. David Wesley is an M.D. and is a vice president of the reinsurance company General & Cologne, where he is involved in underwriting.

Each of these two speakers are going to present their views on risk management for e-commerce. As I said, I think you're going to find their thoughts are very different than mine. Our intent is to stretch your mind and make you aware of the problems that you're going to face in the e-commerce world.

Mr. Steven Tippins: I'm not an actuary and will never even attempt to be an actuary. I took some calculus somewhere and learned enough to pass the class and greatly admire what actuaries do. I've recently started a program in risk management of insurance at Roosevelt University. I've been teaching this stuff for many years and was a life insurance agent early in my work life.

Not only do I teach risk management, but my other unique qualification for this program is that in the last two years I've become a part owner of two Internet start-up companies. Unfortunately, both of these companies are still just worthless Internet stocks.

In relation to Jay's comments about low unit cost being a necessity for e-commerce, it is for this very reason that you're seeing a lot of universities go into "education online, on the Web, e-college", "blackboard", and so on. They're making this move because 50–60% of university cost is brick and mortar. If I can eliminate 50–60% of the cost, and charge the same tuition, educational institutions will make a lot of money. However, the schools are finding that nobody actually takes these courses, or when they do, they drop out. There's a limited market for this stuff, and there will be a limited market for a lot of stuff on the Internet.

My definition of risk management is a systematic identification and treatment of exposures. I used to say exposures to loss, but the field of risk management has gone into holistic or integrated thinking. Many areas do risk management within insurance companies now. There are the traditional risk managers in a firm doing risk management as well as actuaries and investment people. But who cares where or why a firm lost money? Thus, risk management has become what I like to call organizational risk management because the need for risk management is pervasive across the firm.

Risk exposures can be positive and negative. I have problems with undergraduate students understanding this concept. I get them to understand that risk is variance from what you expect, but then they say, we can only lose. I use the example of a cereal manufacturer that packages 18-ounce boxes. If the manufacturer decides to load the boxes with just 16 ounces in each box, for a while, the manufacturer will win, until people find out about the shortage. On the other hand, if the manufacturer is loading 22 ounces in each box of cereal, there is a definite loss. The other problem I have with undergraduate students is they tend to confuse undesirable outcomes with risk. For example, if I hold a gun with six bullets in it and know the gun works, and I pull the trigger, how much risk do I face? Anybody want to try? None! The expected outcome is a big old hole in my head. There's no variance from what you expect. Now, from my perspective, it might be an undesirable outcome, but from the pure risk standpoint, there's no variance. Just because something has an undesirable outcome, it doesn't mean there is a risk; it just means it's an undesirable outcome, and that's something you want to avoid.

The first thing a risk manager needs to do is set the objectives for a risk management plan. For example, does your firm need to be in business continuously, or can it go down for a while and still come back? If you own a restaurant and you go out of business for a while, are people going to wait to eat? No, they're going to find another place to eat. If a life insurance company office burns down, you can probably handle this matter because you'll figure some way to pay death claims and run the business. Sometimes a company's needs are defined by the federal government, such as "thou shalt not pollute."

Another task of a risk manager is to identify a company's exposures to loss. Some risks can even be highly subjective, even incredibly subjective, because what might be a high risk to you might be no risk to me.

Next, risks have to be evaluated. Funky statistics and other estimates size up losses. Be careful not to carry your results out to the 19th place just because the calculator will do it. You will be implying a level of accuracy that you don't have.

Non-Internet businesses risk management plans probably can't be done more often than quarterly. But with the Internet, things are moving so quickly that you might want to be doing some of your planning monthly. I know one Internet firm that works with advertisers on a one-month contract. If there aren't enough hits, it moves on to another relationship because the Internet world is driven by eyeballs or hits. It is imperative to constantly bring people to Web sites.

I want to share some definitions relating to e-commerce that I've seen and liked:

- E-commerce is the actual buying and selling of goods on the Internet.
- E-business is safely working cheaply, faster, and smarter using the power of the Internet.

I would venture to say that most firms are involved in e-business because they use e-mail to speeds things up. On the other hand, E-commerce is a much tougher matter. Even today, I don't see a lot of people running to the Internet to buy life insurance. If they would, then life insurance companies wouldn't be paying huge commissions to agents. I expect that people will go to the Internet to get information.

Economically rational people will search out the lowest price for a product. However, there's still more than one life insurance company offering life insurance and even many forms of life insurance. The reality is that people generally buy life insurance from the people they talk to.

The Internet is being adopted quickly by consumers, but not as quickly as some people say. One of the reasons is that while a lot of people have access to the Internet, they don't know how to really use it. Learning to use the Internet will take time.

A major firm in the Chicago area involved in the insurance industry has said the following about the Internet: "The Internet poses unique problems because of its global reach and digital format. Its phenomenal growth contributes to the confusion by possessing yet unanswered legal and regulatory questions. The entrants into electronic commerce are often unaware of some of the more troublesome aspects of their industry."

With or without the Internet, doesn't that quote describe many of the problems facing both the life insurance industry and other businesses? The point is that managing an Internet business faces many or most of the same issues as running a business before the Internet.

A passive Web site just provides information. These sites tell the reader about the company's products and then say, "If you want more information, call 1-800-xxxx. Trust me, none of us will ever call the number. The Internet has to provide an immediate response. For the Internet to be an effective sales tool, it must work on an interactive basis, allowing the customer to interact with the Web site. At least offer the availability of sending an e-mail message to get more information.

My own move from Washington DC to Chicago is a great example of the value of an interactive Web site. I decided to make use of the Web for the move, and I e-mailed four realtors in the town where we wanted to live. I told them I wanted to buy a house and gave them my parameters.

Only one of the four real estate agents responded. My wife and I e-mailed her back, she called us once, and we flew into Chicago for a weekend look at the properties. The result was we bought a $300,000 house. Almost everything involved with the sale was done on the Web. The key to the sale was the response from the real estate agent. Surprisingly, while several agencies wanted to sell using the Web, only one agent responded to our inquiry!

There are actually some firms offering risk management as a service on the Internet.

The Internet can be dangerous if a firm simply decides to become involved "because everybody else is doing it." This is a defensive approach to Internet participation as opposed to having a reason to be on the Internet. Be careful if you don't have a definite reason for becoming involved with the Internet.

The big problem is identification of problems. The first one is privacy. This problem must scare life insurance companies to death. How does the industry keep the information private. It has been doing it well for years, but now, with the Web and hackers, and everything else, how does the industry keep information private, and still get people to give information to us? People are afraid. Also, as on aside, did you know that 10% of the credit cards used on the Internet are false or stolen?

A second problem is down time. If a person goes to a Web site and it's down, you can be very certain that they're not coming back. If you're going to host your own Web site, you will need redundant capabilities.

A lot of Web sites are putting on, in effect, disclaimers, saying they're going to collect information on you. Some sites even allow for a person to say he or she does not want you to share information.

There are insurance policies to protect against some of the potential Web-related problems. However, on the property and casualty (P&C) side, it seems that the policies were written 100 years ago, and they keep trying to amend them to work with today, as opposed to saying trying to come up with a new policy that is specifically designed to meet today's needs.

Actually implementing a Web site requires a company to make several basic decisions. For example Sears has a Web site, and the goods on the Web site have prices that are identical to those in their stores. They've made a decision not to cannibalize their stores and to use the Web site as a minor marketing piece. It is possible that Sears' concept is to have a customer buy goods on the Web, and go to a store to pick up the items because, it hopes that once you're at the store, you'll pick up something else there.

If insurance companies have agency forces, they face the same problem as Sears. The issue is whether the policies on the Web site are going to be priced to undercut the agency force. About 20 years ago, Hartford and the American Association of Retired Persons (AARP) teamed up to sell auto insurance to AARP members. Hartford's agents went ballistic because they were going direct and potentially cutting out their commissions. The message is be prepared to face this type of conflict if your company operates another distribution channel.

The digital divide is getting a lot of attention now, and it is real. There are a lot of people who don't use the Internet or don't use it effectively. For most of us nontechnical computer users, it isn't necessary to have the latest chip because of how we use our computers. The implication of this fact, for companies trying to communicate with customers using the Internet, is keep in mind that you just have to have people come to you. This is probably accomplished by brand identification.

The Internet is another way to do what you do better. You're still going to be insurance companies, and the Internet's going to be a tool to help you either be in e-business or e-commerce. That's all it is. Yes, it is a global media so that more people can see your stuff faster on the Internet, but they could've seen it eventually.

One thing insurance companies might have to worry about is regulations. On the Internet it is very easy to cross state lines, because the Internet doesn't know where you are when you are on line. Contacts can come from other states and even other countries. For years, life insurance agents have gotten around the state license issues by saying that the applicant signed a form in a state in which the agent and company are licensed. The most recent policy I bought was from my agent who is in Massachusetts. He sends me the stuff I need to sign and says that I signed it in Concord Massachusetts.

Mr. David Wesley: I'm not an actuary, but I frequently eat lunch with actuaries. I am an M.D., and an insurance company medical director. As a medical director, I'm probably most comfortable in talking about a subject such as prostate biopsies. So why should I be talking about Internet issues? I'd like to think it's because I'm the only one in the office who has actually downloaded files onto my calculator. In fact, I am sort of the office nerd for technical things, the Internet, the data basis, and stuff like that.

A year and a half ago I created a reflex questionnaire for obtaining underwriting information off the Internet, and I'm currently changing our underwriting manual from one form of hypertext document to a Web-based technology. So I'm familiar with the Web technology, and what I'm going to be talking about will be in part underwriting, and in part technology, but I hope it is the technology part that you find the most interesting.

My description of the risk management process is very similar to Steve's:

- Identify and analyze loss exposure
- Measure potential loss exposure
- Select a mitigation technique
- Implement the chosen technique
- Monitor and make necessary changes

When I first accepted this opportunity to speak to you, I was planning to talk about risk management issues relating to underwriting, but because there was a whole session on this subject, I am going to blip through the underwriting part of my presentation very quickly. I might have a different opinion than what you heard at the other session.

Many people say that life insurance is the ideal virtual product. After all, there's no need to send a UPS truck out to deliver a policy, unlike CDs and DVDs and other things that I buy over the Internet. On the other hand, it seems like life insurance has become the last frontier. Our industry has been very slow in adopting Internet technologies, and I'm not actually aware of any company making a complete sale over the Internet. Inuity.com probably comes the closest. I learned yesterday, that they still get a signature on paper.

There is a good model for selling insurance over the Internet, and I encourage you to check out a Web site called ecoverage.com. This is a California company. It has been selling auto insurance since February. They seem to be doing quite well for themselves. You may be quite frustrated to try to dial them up wherever you are. For the longest time I could not get on their Web site from Connecticut, but it has been just recently that they have plans to start selling in Connecticut and have allowed me to access their Web site.

I also attended a presentation by the president of eCoverage, and one of the things he bragged about was he was able to reduce the number of questions on the application from seventeen to five. When I go on the Internet, it still looks like there are 17 questions even though he has batched them into five parts. The site

works very well. There is nothing fancy yet it is well-designed and easy to follow and understand. One of the things you might notice on the Web site is on the home page; right under eCoverage there's a subtitle " the industry is history."

This eCoverage provides an instant policy. It does not require paper to be sent to the client. When I attended the presentation, I mentioned that one fellow had a very good question, how do you know that the car is not already damaged? The president was vague at that point and didn't really give any details, but he alluded to third party verification. Using the Web site I got as far as a quote, and then they wanted personal information. They want me to buy before they tell me anything more about what will happen next. I assume there has to be some sort of third party verification that the car is ok. There's no prior damage, and the vehicle identification number has to be verified.

When I bought auto insurance from GEICO, I could do everything over the telephone, but then I had to drive to an office in Darien, and some guy came out, looked at the car, said it's not damaged, and verified the vehicle identification number (VIN).

Mr. Sanford B. Herman: I had to move to Connecticut a little over a year ago and go through the process of registering cars. I found that you have to have paper. It's also required that you have to have these insurance cards in your car so that if you get in an accident, or the police stop you, you can prove that you have insurance. How does e-commerce get around these requirements if they don't provide paper?

Mr. Wesley: I don't know for sure but I think that you could print a certificate on your laser printer. The same thing is required in California too.

Mr. Herman: How then would the certificate you print be guaranteed to be authentic? I'm just throwing out an issue to find out how we can live in a paperless environment when regulation is paper–oriented.

Mr. Wesley: That's a good question for which I don't have an answer.

Mr. Tippins: The answer might be very simple. I suggest a hookup between the insurer and your state Department of Motor Vehicles. Then your DMV can go to a database to check whatever is needed and it's all paperless.

Even when you're stopped for your speeding ticket, the police are hooked up to the DMV directly from their cars. To make this industry work, you need a monster database but that's not unattainable in today's environment.

Mr. Wesley: The large part of the underwriting for auto insurance is done through databases, and I'm sure the first thing they check is the DMV and related databases to make sure you have a legitimate car. As far the document is concerned, and as long as you have the number for the policy, I'm sure that the police can use their laptops in the squad cars and access information about your insurance too. I'm actually interested in this company and I might switch coverage, just to try it out.

I expected that the price would be higher for comparable coverage, but their price is quite competitive.

I've heard of home insurance also being sold in the same way but I can't give you a name of a company.

On the other hand, what is required for underwriting individual life policies is more involved. A life insurance application might look like it has 20 questions, but if you look at part B, each question has five or six subquestions within it, and you end up with almost 100 questions that are being asked. We also have MIB authorization.

It used to be that the MIB authorization had to be signed on the paper copy in order for the insurance company to access the MIB, but just within the last month we relaxed this rule, and if the insurer is willing to assume liability for it, MIB will allow the insurer to access their database with just verbal authorization. This is something that has happened without a lot of discussion that I'm aware of, and I'm not totally comfortable with, but it certainly facilitates doing on-line insurance sales.

The most important tool the underwriter currently uses is the attending physician's statement (APS). This is also the tool that slows down the underwriting process the most. When you hear of cases taking 100 days to go to issue, it's usually because the underwriter is waiting for various attending physician's statements.

Unfortunately the APS, in my opinion, is deteriorating rapidly in it's quality. It used to be that doctors would level with us. When they weren't willing to give us that information, they would provide us complete records for the underwriter to sift through. What I find today is that doctors are removing pages from the APS, not recording information about a patient visit, and, in some cases, I've actually heard that doctors are advised to keep two sets of records—one for insurance companies and one for taking care of their patient. So I don't think the APS is what it used to be, and for reasons other than just doing business quickly over the Internet, I think we should be looking for ways to underwrite without APSs.

What is most important in Internet sales is a positive customer experience. Those that are successful in selling over the Internet make it as easy as possible. Internet buyers want things now. They want lots of information. They want to control this process and decide for themselves what they're buying and why they're buying it. They also want to pursue the sale in total anonymity up until the point where they actually give you the credit card. Of course, you're looking at privacy issues as Steve has emphasized.

A couple of speakers mentioned that the placement rates for Internet sales are not very good. I find that very easy to understand because the way I and other people shop on the Internet is to try things out. We go to a Web site, we see how it works, but because we have never used it, we're suspicious. I'm not going to give out my credit card number until I'm totally comfortable with a Web site. So I go through the whole process and go to the last point to see what they're asking for. I'll come back to it later if I really want to buy the product at the Web site. Then I

go and shop somewhere else at that point. If I still want to buy something, I'll go back to the one where I was most comfortable, and make my purchase on that site.

One instance of sales over the Internet that is available right now would be through sites where the human resource departments have set up a Web site to handle all the questions about benefits and the sales of additional coverage, such as supplemental life insurance. These are increasingly popular, and I expect to see more and more of these in the future.

I'm going to make a prediction that eventually the Internet will be a good vehicle for selling life insurance but first we will see offerings along the lines of eCoverage, where there's simplified underwriting using databases that are easily accessible. Such databases include motor vehicle reports, credit reports, and drug usage information that is available through certain databases. My impression is that these channels of distribution will never be able to support the price that one gets through more complete underwriting. This probably means that some companies will still be able to offer cheaper life insurance through the use of a modified, improved underwriting process as compared to what's now being used.

The Internet will be used to help facilitate examination appointments. There even might be an opportunity for computerized medical records, although computerized medical records are a long way off. Because of privacy concerns, it will be quite a while before we see them used for this or any other purpose.

There will also be some sort of distributive processing. This can be as simple as what we currently have through the insurance labs where the insurance lab has our programs as to when we want reflex testing based upon age, face amount, or some other lab results.

Now I want to talk about privacy. The medical director in direct writing companies is often responsible for privacy issues. The medical director is the person who handles cases with positive HIV results and other sensitive matters. We are the liaison for MIB. I'm also interested because of the problems with APSs. As I mentioned, attending physicians are providing less and less information. They do this largely out of privacy concern and a misguided impression that this is actually acceptable. They think it is acceptable to lie to the insurance company because they are doing it for the patient.

I looked hard for definitions of privacy, which, when you think about it, is not that easy to define. A very popular definition is anonymity. When it comes to selling though, or buying as a customer, anonymity is usually reserved for those who enter a store with a mask over their face. A better, more workable definition is to have control over your personal information. Another definition is the Supreme Court definition, which is the right to be left alone.

Confidentiality is often confused with privacy. Confidentiality is different in that when the person decides to share information with us he or she expects that it's going to be handled in a confidential way. In other words, it is not going to be

made public. The opposite of privacy is identification, which is something a lot of people don't think about.

It was not until very recently that the life insurance industry required photo ID's, such as driver's licenses. It was when testing took off, and the problem ensued with trying to match up test reports with the insured's policy that examiners started to ask for driver's licenses or other forms of a photo ID. It's remarkable that that never happened before.

I'll discuss a little bit of technology pertaining to how the Internet works. The Internet is very open. When Steve or Jay logs on to the CompuServe site, they are actually connected to my computer, and if I knew which internet provider (IP) address CompuServe gave Steve, I could actually probe his computer and look for files. When you're using the Internet, you have a browser in your machine, and you're connected through the Internet to any other Web server out there. Your browser sends a request to that IP address, the Web page, for information. The Web page is downloaded to your computer in what is called a client/server relationship. It shows you information; you're a client of that server. The PC peripheral interchange program (PIP) protocol calls for the request and/or the information being sent to you to be broken up into little pieces, and each piece is labeled with an address. It's as if the server says, "You go to Jay's computer now," and each piece goes off and takes whatever channel is available to it. There's a great feel of redundancy in these packets. They're called, sent through whatever channels are available to them, and at the browser, it is rearranged. It is like putting back together pieces of a jigsaw puzzle. He creates the Web page.

Sniffers are able to access information that's being sent at your information service provider (ISP), which is your Internet server, like CompuServe, at the Web servers ISP or anywhere along the backbone. Sniffers are pretty simple to conceive if they're strictly like telephone lines. Hackers are able to find their way into the Web server to obtain confidential information. Most servers are maintained at a site other than where the developers do their work to create the Web pages and to do other information that's found on the Web server. The developers access the Web server through a password. They have privileges to make alterations, view the data that's on the Web server, and access that information that way. Hackers are able to get around the password protection and have free reign to either look at the information on the server or change it.

"Man in the middle" attacks are interesting. It is possible that, as Jay is using his browser, he is sending a request to the Web server that he is interested in, but somebody is in between him and the Web server posing to him like a Web server and posing to the Web server like a user. Hackers are able to alter information to their advantage.

One thing I didn't mention was denial of service attacks. They made a lot of news lately. There were some major sites that were brought to their knees by denial of service. The one thing I have to say about it is there is no good way to prevent denial of service attacks. Denial of service is where the hacker is able to pose as

many, many users and access your Web server thousands of times and overload it's capability, and prevent other legitimate users from accessing that server.

So I propose that the real risks of doing business over the Internet relate to privacy and confidentiality issues. There is a great deal of reputational risk and some real litigation risk in the liability of handling information. There's also opportunity for fraud. Those who know how to manipulate data can change contracts and other terms of insurance when sent over the Internet. The last risk is poor underwriting information. If you're not able to identify the information as belonging to the person being underwritten, it might not apply.

I'm going to talk about some ways to moderate these risks. Digital encryption, in particular, thwarts sniffers. There are secure Web servers that use encryption and encryption techniques to prevent data from being given out to hackers. Finally, and probably most importantly are digital signatures. As someone mentioned at another session, there was a law passed by both houses last week that enables the digital signature to be used for contracts in the United States, and I'll talk more about this later and give a few details.

It's my opinion that the digital techniques are used for encryption and digital signatures will become pervasive not only over the Internet, but in other ways. Written signatures have their weaknesses that encrypted and digitally signed documents don't have.

Cryptography works and is feasible thanks to computers. Computers are the basis of the Internet. Only computers are able to handle the concept of documents as large numbers, and the complicated algorithms that encode and decrypt documents. I'll go through encryption to show you how it works.

Public key cryptography is very important. Hashing is when a computer will look at a document (the series of characters), as a very large number, and convert it to a smaller number, say 128 or 160 bits or whatever you choose. This smaller number serves as a fingerprint for that document. One of the rules for a good hashing algorithm is that any change to the document will result in changes to the bits of the hash or the digital fingerprint. This enables somebody to make a small fingerprint of the large document and compare that to another document that has been signed digitally. They should be able to tell if a document has been changed, which would make it nonreputable.

Encryption is simply taking plain text, converting it into a cipher text. Decryption is converting it back to plain text. It requires a key and an algorithm. All the security is in the key. The algorithms are publicly known. Symmetric encryption, the same key, will both encrypt and decrypt the message. This kind of technique can be fast and straightforward. It can be so fast that you hardly notice it. If you use secure sockets on your Web browser, you're using encryption. It slows down a little bit. You can notice it, but it's not terrible. The only problem is how to share the key.

Encryption works using an XOR function. The computer sees all numbers in binary form. If I wanted to send a message to Jay and I just had the first two letters, J A,

I could use this as my encryption key. The XOR function is just a combination of these bits and the rule for x-or is one or the other but not both. We have both and it comes out as zero. The decryption operates the same way. If you XOR the encrypted message using the same key, it comes out with the original. XOR functions are very trivial for someone to break. They aren't very secure.

Real encryption techniques such as data encryption standard (DES), which is one of the most commonly accessed ones, use 16 rounds of XOR, permutations, expansion, compression, and some people use triple DES, so they'll do it three times. In public key cryptography we have a different matter, and this is very important and very clever. The keys are arranged such that there's a public key and a private key. You could have a private key, such that the person who wants to send a message publishes his public key so that it's available to anyone that might receive the message, but he encrypts it with his private key. The public key can decrypt it. What's interesting is that you can't decrypt it with the private key, which is one of the features of this kind of algorithm.

Unfortunately, it's relatively slow, and in practical use you'll see it used to encrypt the key for a regular DES transmission. This is a black dart diagram showing how a digital signature would work. The message, the document, whatever is hash, and there's a hash result. There is a signing function that is used to XOR, the hash with a digital signature, which again is another large number. The message and the digital signature are sent using a private key. The recipient takes the message, decrypts it using the public key, and the message part is hashed again. The hash result is verified by comparing with the decrypted digital signature hash.

Signatures provide evidence or a ceremony, and there's a certain weight that is associated with putting your signature on a document The opening tags and the closing tags identify the digital signature as a promissory note. The opening tag and the closing tag identify this as a digital signature. The computer that receives this knows what to do with those elements. Within the opening tag of the signature we have the public key ID so that the computer knows where to go and where to look for the public key for the signature.

I have a few more details about the Digital Signature Act. This was also known as the Abraham Bill, and it's not the first act for digital signatures. We've had digital signatures at the federal level. There were acts in 1996 and 1997, and several states have their own acts. Congress was trying to correct something that was wrong with some of the original acts. The business model that these acts called for was one where a certified authority was, for a fee, to provide assurances that the digital signature corresponded with the person. Nobody really wanted to do this. There's no company that is doing this on a large scale except Verisine and it mainly works with the digital signatures of software.

This act allows parties to agree among themselves upon a certified authority and what will constitute a digital signature. Actually, the act refers to electronic signatures, which is not necessarily a digital signature. If any of you have submitted your taxes this year to the IRS and signed it with the eight-digit number

that it gave you, that's an electronic signature. It's not very secure. Anybody could've taken that number and used it, but that's the way it does it.

This is where I make a case for a role for the actuary. Digital signatures and encryptions are mathematical techniques. There is nothing absolute about them. Any digital signature or any encryption that can be decrypted can be broken. It's just a matter of estimating the likelihood, and weighing that against the cost of using such techniques. This seems like an ideal task for an actuary.