Internet Insurance Whitepaper How to Build Insurable Internet Business*

by Steven B. Adler and Richard A. Sand**

1. Introduction

For centuries, insurance companies have played a pivotal role in determining the insurability of products. Building construction materials, car parts, planes, trains, ships, consumer goods; almost every product used for commercial purposes today has been sanctioned, in one way or another, by an insurance company. In many cases, insurance companies have worked with state and local governments, with consumer safety organizations, and directly with companies to establish building codes, auto safety features, and consumer protection legislation.

The goal for insurers has been to reduce risk. Consumers have been the main beneficiaries, but companies also benefit. Insurable safety standards level the commercial playing field, creating a stable and secure marketplace.

On the Internet today, there are no insured, or sanctioned, standards for security. Business on the Internet today is like gold-panning in the Wild West – all the risks are borne by the adventurers. In the real-world, no businessman would open a new enterprise if an insurer said, “swim at your own risk.” But today, millions of businessmen are Web’ing up to do just that.

* Paper presented to the 12th MORE Seminar of the International for the Study of Insurance Economics, Winterthur, 1997.

** EMEA Network Computing Managers, Insurance ISU, IBM Denmark.

Internet Insurance can change that. By assessing commercial risk on the Internet, insurers can make that environment stable and secure. They can establish Internet security construction codes, transaction encryption standards, and let market forces – premiums and losses – dictate the winners and losers in the battle to secure the Internet for commerce.

But to offer insurance for Internet commerce, insurers will have to become intimate with the Internet. They have to learn to speak the Internet language, in all its strange and foreign dialects. That is where IBM can help. IBM has developed a methodology, called Net Risk, which provides a blueprint for insurers who want to underwrite exposures on the Internet.

As the world's foremost network computing company, with more than 30 years of network security experience, IBM knows the Internet fluently. IBM can help insurers understand how to identify Internet risks, reduce loss exposures, and underwrite the Internet as a profitable new line of business.

In the process, IBM can take the entire discussion of the Internet and Insurance out of the basement – where we sell firewalls, servers, and web services to IT – to the boardroom, where corporate decisions are made. This service initiative will empower insurers to influence the growth of Internet commerce, allow companies to insure their business on the Internet, and IBM owns the patents, skills, and resources to do it today!

This White Paper will demonstrate how insurers can secure Internet commerce, using the analogy of an on-line merchant building an Internet business. We will show how the merchant can build an Internet warehouse to effectively deter hackers, protect valued inventory, and deliver products securely. And, we will demonstrate how the Net Risk methodology can help insurers turn the analogy into reality.

Along the way we will explore some fundamental relationships of commerce, as well as some of the underlying technologies of the Internet. We will then turn to the insurer's perspective, demonstrate their business opportunities, illustrate online exposures that correspond to traditional insurance lines of business, and highlight IBM solutions.

1.1. Building a warehouse on main street

A retail book merchant wants to expand his business and open a direct-mail channel in another city. He studies the new city's demographics, locates shopping malls, and identifies traffic patterns. Based on an analysis of available building sites, the merchant chooses a large plot at the end of a shopping mall, near a major road. The site is large enough for a warehouse, has accessible parking, and is visible on the road. Additionally, the neighborhood is in a low-crime zone, has good police and fire protection, and a local security firm watches over the shopping mall.

After hiring an architect, the merchant prepares for construction. A foundation must be laid, boilers installed, plumbing pipes routed, electrical lines put in. Walls, floors, ceilings, doors, windows, fixtures, and equipment will be installed. Door locks, sprinklers, a fire escape, a ramp for wheelchair access, burglar and fire alarms, security cameras, and other devices will secure the exterior against break-in or damage.

When the warehouse is complete, the merchant will purchase inventory from a variety of publishers, advertise a grand opening, and begin business. Orders will arrive via post or telephone, and books will be shipped out the same day via UPS.

Should a DC-10 crash into the building the next day and destroy everything, the merchant will be heartbroken but not out of business. His walls, floors, ceilings, doors, windows, fixtures, equipment, and inventory are all insured. If the DC-10 also destroys the UPS delivery truck being loaded outside, all the parcels are insured against loss or damage in transit.

1.2. Building an electronic storefront on the internet

Instead, if the merchant chooses to open an on-line book warehouse on the Internet, and a HackerC-10 breaks through his firewall and formats his data warehouse, the merchant will be heartbroken and penniless. If the HackerC-10 also manages to intercept a stream of outgoing book orders, crack the credit card codes and steal all the documents, the merchant may also be subject to liability suits from his customers.

To protect against this type of damage, the merchant needs to build a very secure electronic warehouse. From the foundation to the roof, she needs to consider every facet of the building's architecture. If there is any flaw – sloppy mortar between the foundation stones, loose panels in the walls, poor fitting window joints, or bad plumbing – a hacker will discover it and use it to his advantage. So the building has to be top-to-bottom secure, and that standard demands an architect with world-class credentials.

But before we draw up the blueprints, let's first examine the purpose of the warehouse and its special needs.

Figure 1

2. The Building

The most important qualities of a well-built Internet warehouse are the same as a real-world warehouse:

- 1) *The warehouse is built properly.* The computers must be highly stable and fault tolerant, and the software (operating system, network software, and applications) must be rock-solid secure.
- 2) *The warehouse is monitored properly.* A comprehensive systems management solution monitors for attacks and other faults, alerts administrators, and reports on activity.
- 3) *The warehouse is enforced properly.* The network is programmed to actively defend, and identify and deter aggressors. It must shut itself down if it detects a security breach, and provide a detailed audit trail.

Let's examine the design of the book merchant's electronic warehouse, keeping these three qualities in mind.

2.1 Structural integrity

When describing the structural integrity of the electronic warehouse, we must identify what makes an electronic presence on the Internet structurally sound. We use the phrase *structural integrity* loosely, for we are in fact discussing the entire planning phase of the warehouse. This includes choosing the location, the design of the building, and the planning of business operations.

2.1.1 Warehouse architecture

A building must have a solid foundation. In computer terms, this means running on a good hardware platform. Computers that provide service to the Internet are typically high-end machines, such as IBM S/390, SP2, RS/6000 or AS/400s. These machines are designed to process large volumes of data, and are built to be highly resistant to failure. Machines of this nature are prerequisite for a properly designed electronic warehouse.

An Internet warehouse performs many different tasks, so multiple computers are needed to perform specialized functions. Specialization enhances security. The *firewall* divides the network into three areas – the internal (intranet), the external (Internet), and the *demilitarized zone* (DMZ) – and secures communication between them. The database server, the heart of the company, resides in the internal network. The web server sits in the DMZ processing requests from users on the Internet. And the transaction gateway handles the interaction between the web server and the database server.

Each server requires the most sophisticated design for high-availability. This means having a parallel machine as a “hot-standby”, storage technologies such as *mirroring* or R.A.I.D, and multiple links to the internal network.

2.1.2 The warehouse location

Just as important as the strength of the building, is the location of the building. A well-designed warehouse must have a well-selected location. In Internet terms, this means selecting a quality Internet Service Provider.

A good Internet Service Provider (ISP) can provide good access to the Internet (called *bandwidth*), has reliable technical support, and has sufficient resources to offer high availability. Selecting a poor ISP is like building the warehouse in the inner city: road access is poor, and the local police can't deter crime. The poor ISP gives low-quality or sporadic bandwidth, and cannot adequately prevent hackers from hacking in the ISP's network territory.

2.1.3 Warehouse operations

In the electronic warehouse, the jobs involving operations are done by software such as IBM's *Net.Commerce*. The software manages inventory, processes orders, checks credit-card authorization, records transactions, and handles delivery.

The electronic warehouse and the "real world" warehouse overlap strongly at this point, because these functions of the business are computerized for both. Orders, inventory, and invoices are all stored electronically on computers with special *databases*. For the "real world" warehouse, a person must check the computer database for the order, and print out the invoice. In the electronic warehouse, the warehouse software checks the database directly.

2.1.4 The firewall

A firewall is a special computer that sits between the company's internal network (intranet), and the Internet. The firewall is the front door to the network. Because the Internet is public, any Internet user can send information to your network. On the Internet, information is broken down into small messages called *packets*. The firewall uses *packet filtering* to decide what packets are allowed in and out of the firewall.

The network administrator decides what packet filters to use, to allow only the desired traffic. If an Internet user tries to issue a command to your web server, using a standard program such as *rexec* (stands for *remote execution*), a properly configured firewall will refuse to deliver the command. But if the Internet user tries to connect to the web server with his Internet browser, then the firewall allows this connection.

The firewall also hides the company's intranet topology from the Internet. If a hacker doesn't know that a database server exists, then there is nothing to hack. Technologies like *Network Address Translation* and *SOCKS* allow the company's employees to safely use the Internet from behind the firewall, without revealing information about the company's intranet. The firewall acts as a go-between, called a *proxy*. It receives requests from the intranet, and forwards them to the Internet. From the Internet's perspective, your company's network consists of only two machines: your web server and your firewall.

Today's firewalls also provide a service called *secure tunneling*, which allow sensitive transactions to take place over the Internet. A secure tunnel is a special connection, over which all data flowing between two machines is encrypted. The protocol for establishing secure tunnels has been standardized, so any vendor's firewall can set up such a tunnel with any other's. Secure tunneling allows the intranet database server to verify a customer's credit limit, or allows network administrators to work with the web server remotely. If someone on the Internet tries to eavesdrop on the secure tunnel, all they will hear is static.

2.1.5 The web server

The web server distributes queries and replies between servers on the intranet and clients on the Internet. A web server relies on encryption algorithms to secure the data flowing through it. Encrypted client requests from the Internet pass through the firewall and are brokered by the web server. Reply messages are also encrypted out to the Internet.

The web server allows access to an intranet database server. The web server processes queries, and using a technology known as Common Gateway Interface (CGI), passes it to the database. The web server then passes the reply back to the customer. At no time has the client directly accessed the database computer.

Encryption algorithms today are based upon a mathematical function using two large prime numbers, which serve as keys. The first key, called the *public* key, is used by the web browser to encrypt the information so it is unrecognizable.

The encrypted data is then sent through a web server to the transaction system. This secure internal machine has the second key, called the *private* key, which it uses to decrypt the information. Even if a hacker gets the encrypted information and the public key, he still cannot decrypt the information without the private key. This provides the entire mechanism of secure electronic transactions for the public Internet. It enables electronic warehouses, home banking, and other sensitive transfers to occur safely over the Internet.

2.2 Protection and enforcement

The second point addresses the protection of the warehouse and the third addresses protection. They are combined here because they go hand-in-hand. A good protection system must be backed by a good enforcement system. A security alarm without police, or a smoke alarm without a fire department, is a useless alarm.

Protection and enforcement of a network are achieved by *Systems Management*. System management means keeping operators and network managers informed on the state of the managed machine (the firewall, and the other machines that comprise the company's Internet presence).. This is carried out in three ways:

- 1) *remote monitoring*- allowing a centralized management system (one or more) to watch the managed machine and query it for status information.
- 2) *automatic alerting*- enables the managed machine to send unsolicited messages to the central management system, usually to indicate a problem or warn against a possible problem.
- 3) *reporting*- allowing the centralized management system to generate meaningful activity reports continuously, so the health and security of the managed machines can be evaluated.

One of IBM's greatest advantages in the Internet world is our ability to provide robust system management of and through a firewall. *Secured Network Gateway* (IBM's firewall product) and AIX (the IBM operating system that SNG runs on), in conjunction with IBM's system management offerings (TME10), provide powerful systems management facilities.

2.2.1 Remote monitoring

Monitoring starts with checking that all of the systems are up and running OK. We begin by monitor for the health of the hardware and software (with products such as SystemView Systems Monitor or Tivoli Sentry). Additionally, we must also monitor for intruder attacks (with offerings such as *Firewall System Management Package* and *Web Server Security Package*). And if an intruder attack occurs, we must decide how our network will react.

The facilities of AIX and SNG provide a detailed audit trail of all system activity. This audit trail is then studied by special analysis programs, which are the equivalent to security cameras. Any irregular findings in the audit trail are reported.

Some examples: a critical system configuration file is altered (a hacker, or even an employee, has broken in and is trying to achieve a higher security clearance by changing the configuration). A user tries to log in with the wrong password too many times (a hacker is trying to guess a password). A machine on the outside is using an address that is reserved for the internal network (this form of attack is called IP-spoofing). Someone on the outside probes the firewall with disallowed “unsecured” network services (remote login attempts, remote execute commands, or special hacker software such as Satan 1.1).

2.2.2 Automatic alerting

After a system management program detects a problem or an intruder attack, the network can react in a variety of ways. It can create a report of the problem, send an administrator mail, generate an alert to a central management system, execute a program to take automatic corrective action, or any combination thereof.

Lets say that a hacker has tapped into the network cable running between the two of our electronic book merchant’s corporate offices. This hacker then sets up his own computer on the cable tap, and tricks the network into believing he is part of company. First he listens to the information flowing across the line, to hear which systems are talking. He then begins to mimic them, carefully probing through the network. Finally, he discovers our electronic warehouse system. But since he has tapped directly into the internal network, he has bypassed the firewall! He sees a golden opportunity to steal valuable information (books or software). So, he logs onto the computer holding the electronic warehouse...

Elsewhere in our network, a computer running systems management applications is monitoring the electronic warehouse, and the firewall. And it sees someone accessing the electronic warehouse. But this access is coming from the secure network, and the particular source address on the internal network is not supposed to be using the warehouse! And it is the middle of the night, when *nobody* is supposed to be doing administration! The managing computer reacts. The following happens:

- 1) The managing computer picks up its modem, and dials the network administrator’s pager. It sends the pager a message “Warning! Unauthorized use of the electronic warehouse!”
- 2) The managing computer sends a message to the electronic warehouse, telling it to shut itself down due to an emergency situation.
- 3) The electronic warehouse is shut down.

2.2.3 Reporting

We have already benefited by having a powerful systems management solution installed on our network. The hacker has been thwarted. But was any damage done before the electronic storefront was shut down? How did the intruder get in? Auditing and reporting will tell all. Let's continue our example:

- 4) The administrator rushes to the office (or accesses the network by remote, using a special, encrypted access mechanism such as SecureNet ID Cards) and analyses the audit trail.
- 5) He determines that someone tapped into a cable somewhere and *spoofed* the identity of another machine. An investigation reveals that the hacker had broken into the cable switch box between the two buildings (yes, this does happen!) and had done his work from there with a powerful laptop computer, and a home-built interface.
- 6) The administrator corrects any damage done (again using the audit trail) and adds additional security to prevent this type of attack from happening again. (For example, programming the hard-coded addresses of all of the network interfaces into his network devices, so that they ignore any information from a machine that doesn't have a proper hardwired 12-digit address).
- 7) He thanks himself for implementing an IBM systems management solution.

3. The Inventory

As a technology leader, at IBM we see the Internet as an evolving technological phenomenon, a paradigm shift that is happening all around us. But inside the shift, one paradigm of commerce remains undefined: property. Without an universally accepted definition of Internet property, it is hard to insure Internet Commerce.

Lets go back to the book merchant and his real-world mail order business. An order for a book from a foreign customer arrives. The book is packaged and sent via a global delivery service. The package is insured against loss or damage. If the package is lost in delivery, the insurance company will indemnify the merchant for the book's full value. The merchant, informed of the book's loss, will purchase a new book from the publisher and re-send it to the customer.

This is a commonly understood commercial relationship. When a customer purchases a book, she purchases a physical entity for which there is an agreed upon value. Upon receipt, the customer owns the book and requires no further proof of ownership. Ownership is conveyed in the purchase agreement. The book can be lent to a friend, given to relatives, or sold to a secondhand bookstore. It is a real-world, physical entity with commonly accepted real-world benefits, and limitations, of ownership.

In the cyberworld, digitalization blurs commonly accepted commercial relationships. A document sent by a merchant to a customer via Internet electronic mail can easily be duplicated and resent if the original is lost in transmission.

A digital object that can easily be duplicated and transmitted en masse has no intrinsic value. A dollar has an internationally accepted value based largely on the aggregate supply of the currency in circulation. A dramatic surge of dollar production will

inflate circulation and devalue the currency. Severe overproduction of any currency leads to worthlessness. On the Internet, duplication has the same effect, rendering digital property ubiquitous and relatively worthless.

An object that can be easily duplicated, has no value. If the object has no value, ownership is ephemeral, and insurance can't be applied. Thus, today on the Internet, transactions involving unrestricted digital content can't be insured.

3.1 Securing the inventory

Cryptolopes can change that. Cryptolopes are containers that encase digital information, software, or products with a protective, encrypted shell. Like a delivery package, the encrypted object has an envelope jacket that describes the contents, and identifies the sender and recipient. Also on the jacket is a purchase form. When filled-in and transmitted to the owner, the owner sends back a return-receipt with an encryption key, which unlocks the encrypted container and permits access to the contents. If the buyer sends the cryptolope to a friend, the friend will not be able to access the contents unless she fills-out the purchase form and obtains a key from the owner.

In use today on InfoMarket, cryptolopes are already a commercial success. Widely hailed throughout the publishing industry, they were created by IBM to form the foundation of a new copyright protection system for content distribution. If an author wishes to publish a document on InfoMarket, he can use a cryptolope container to specify the transaction properties of the document. Readers can then purchase the document, and royalty payments are transmitted back to the author, via InfoMarket, depending on the distribution rights assigned to the cryptolope.

The unique properties of cryptolopes endow them with the ability to preserve value and persistent ownership rights. By enumerating distribution rights on the object's "envelope," and protecting against unauthorized access, cryptolopes endow digital content with the same properties as their real-world counterparts – thus they can be insured.

3.2 The cryptolope container

Basically, a cryptolope is an encrypted file. If a browser wants to buy a book from the merchant, a click on a link downloads the cryptolope file to the browser's computer. She has the object but can't get at the contents without first completing the purchase form stored on the cryptolope. Once completed, transmitted back to the merchant, and approved, she now has access to the contents of the file, as enumerated in the distribution rights. If she wants to send the book to a friend, she sends the cryptolope file and the friend has to complete the same process.

Cryptolopes are like bulletproof, microchip encoded, glass object containers with some very special capabilities:

3.2.1 Encryption

The cryptolope uses layers of encryption that prevent unauthorized users from gaining access to the document. An abstract of the object's contents is viewable from the container's jacket, and the encrypted object can be disseminated freely.

3.2.2 Distribution rights

An author can assign the object with properties governing access permission, costs, document restrictions, print and reproduction control, modification rights, depreciating value, resale conditions, notarization rights, and payment privileges that are persistent for the life of the object. Ultimately, even the life span of the cryptolope protection can be assigned to the object.

3.2.3 Fingerprinting

Touch the object, and your digital fingerprint is permanently recorded. That means that the e-mail address, and perhaps the mail server and IP address, of anyone who downloads or receives the cryptolope is stored in a data container on the container object.

3.2.4 Watermarking

In a paper document, a watermark is a translucent design embossed or pressed into the paper that can only be seen when the page is held before a light. In a digital document, it is a faint background image superimposed on the document that preserves the document's copyright.

3.2.5 Metering

Information contained in the cryptolope object can contain pointers to different financial clearing houses. A browser on an online library may wish to read several pages of a naval document. Reading the pages costs \$2. The cryptolope contacts a credit-card-authorization clearing house and received authorization for the \$2 payment. A royalty is then paid to the author of the document, and transaction fees are split between the library, credit card company, and, perhaps, IBM.

Metering can be used to depreciate the value of access rights to an object's contents over time. To assess the value, the cryptolope has time rights embedded in it as an object property. The cryptolope then has the ability to "phone home" to the author to check the object's present value after a period of time.

To ensure scalability, the system won't actually "phone home" with each new object, but will maintain credit authorizations, digital cash certificates, or stored money in various protected purses on the customer's desktop computer. The system will "phone home" principally when these purses are exhausted and more credit or money is required.

When "phoning home", the rights management system will also report usage information, such as the number of times the container was opened, the number of pages printed, and so on. The clearinghouses will convey usage information to rights holders along with their share of the royalty information. To protect the privacy of individuals or the confidentiality of enterprise information, the usage data can be aggregated or made anonymous before it reaches rights holders.

3.3 Insuring a cryptolope

When an Author uses Cryptolope technology to transmit his documents, the Cryptolope can be easily reproduced, but the contents can only be read after a purchase

contract is filled-out, payment has been made, and a return-receipt has been received. The Cryptolope preserves the intrinsic value, assigned by the author, of the original document.

Cryptolopes can be used to “contain” anything. With secure contents, enumerated transaction rights, and insurance, cryptolopes could become the arbiters of value on the Internet.

If our online book merchant has purchased his books as digital cryptolope objects from a variety of publishers at wholesale, the merchant has stocked his warehouse with non-replicable digital objects with persistent value – he has an inventory. The inventory has a value that is insurable, just like a real store. If the merchant is robbed, an inventory list can be produced to assess the value of the loss, verified by the publishers, and an insurance company can make an accurate claim assessment report

3.4 Cryptolope inventory

With cryptolopes deployed to secure inventory contents, new commercial distribution opportunities can be employed. The IBM Infomarket division has written extensively on the economies of Super Distribution, and more information on that subject can be found at <http://www.infomarket.ibm.com>. We will cover some distribution topics in the next chapter, but will focus here on some of the items that could be insured in inventory using IBM Cryptolope technology.

3.4.1 Books

An author publishes an online book. He sells a publisher a cryptolope with the right to make 20,000 copies in the first run. The publisher distributes book objects to retailers, and each object can be reproduced 20 times. At each stage of reproduction, the object has a value that can be insured.

3.4.2 Compact disks

Every time a song is played on the radio, in an elevator, at an aerobic studio, or in a store, there is a royalty paid to its author. Copyright protection agencies such as ASCAP and BMI market this privilege aggressively across the world, ensuring that music authors are not robbed of their royalties when people use their work for commercial gain.

Internet bandwidth is growing daily, and online CD sales are not far away. With more bandwidth, a music CD could be downloaded and burned into a PC CD-drive in minutes.

Cryptolopes can help extend the royalty collection efforts of played music into the digital realm of distributed music. If every digitally transmitted CD is encrypted in a cryptolope container, each music publishing company can choose its own distribution methods. A digital CD object may be granted reader access only. Or the publisher may allow the owner to copy the object and send it to someone else, who in turn pays a royalty to the publisher. The music CD objects sitting in a distributor’s Internet warehouse will be fully insurable.

3.4.3 Gift certificates and rebates

Online stores may entice browsers to become shoppers with digital giveaways, rebates, and gift certificates redeemable at point-of-electronic-purchase. These certificates would essentially be pointers to a database, forms of electronic cash, or online gifts. The issuing merchant has a lot to lose if they are stolen, so he issues several hundred and wraps them in cryptolope containers. Since the certificates have a value, they should be insured.

3.4.4 Confidential information

Medical records, X-rays, CAT Scans, MRI Images, pharmaceutical prescriptions, corporate financial records, pending patents, contracts, titles of ownership, and deeds are all examples of objects of value that can be protected by Cryptolopes. And if they can be protected, and their value can be ascertained, they can be insured. So, for the first time, companies, institutions, and individuals can lock up their digital information in transportable, encrypted, object containers and have the containers insured as if they were steel containers waiting in a dockyard to be shipped across the ocean.

4. Net Risk

The Internet is an extension of the real world by other means. Internet Insurance is thus an extension of real-world insurance to cover online exposures. To understand those exposures, we need to first understand how businesses are using the Internet today and those uses can be exemplified to demonstrate exposures. To facilitate this process, IBM has developed Net Risk, which is a methodology for classifying Internet exposures by activity.

If an insurer wants to insure a car she needs to first understand what is the make, the model, the year it was built, its repair history, driving history, and last inspection date.

Figure 2

This information provides a profile of the car and its driver as risk that can, or can't, be insured.

Net Risk addresses Internet Security from two perspectives; first, by defining a standard for building secure Internet sites; and, second, by defining a methodology for assessing existing sites.

4.1 *Classifying risks*

Net Risk provides the same level of classification by identifying generic Internet activities:

- Internal Publishing
- External Publishing
- Messaging
- Database Access
- Order Entry
- Electronic Commerce

Figure 3

4.2 *Architectural components*

Each activity has unique security requirements, and Net Risk defines the necessary architectural components, and their configuration, to protect the integrity of the online environment, individually and culmatively. Individual components are evaluated and rated, configurations are compared for security effectiveness. Software issues related to

Java, Plug-ins, ActiveX, server operating systems, demilitarized zones, and gateways are explored in detail. Architectural diagrams, tables, and charts describe how the components should be installed and configured for each activity.

4.3 Human policies and procedures

But servers, firewalls, hardware and software are only components in security. Human beings are the weakest link in any secure environment. Like security cameras on the front door of an office building, if no-one watches the security monitors, the cameras are useless and anyone can walk in the front door and steal something. Human policies and procedures are needed to define how to use the components and prevent unwanted intruders from gaining access to sensitive information. Net Risk defines these policies for each activity and shows companies how they need to protect themselves against Internet attacks with more than just firewalls.

The result is a prescription for the best Internet security money can buy, and the standard set is now being used to define an IBM standard for environmental security that insurance industry sanction will help to proliferate. Net Risk defines an Internet Security benchmark that should be used by IBM globally to build secure electronic commerce environments that can be insured. The standard helps to reduce risk and prevent Internet losses, and its adoption tells insurers the site conforms to the highest levels of security and can be insured.

4.4 Known perils

Moving one logical step beyond the benchmark, Net Risk further defines the different types of perils that can hit any one of the above categories of risk. This list provides insurers with an important means for determining coverage and premium. Knowing what can happen is an important first step to deciding what to cover and how much to charge. Net Risk has identified over 65 online perils; from denial of service attacks to SYN Flooding, from spoofing to simple telephone con tricks. Hackers today use a variety of methods to gain access. A site is not safe if the masters are not aware of the threats.

4.5 Net risk audit methodology

With the standard set, and the perils known, it is now possible to compare existing Internet sites to the Net Risk benchmark. Net Risk further defines on-site audit procedures which provide insurers, and customers alike, with a standardized audit report. The results of the audit can be used by insurers to define risk and premium, tariff discounts or charges. And it can be used by customers to determine security strengths and weaknesses.

Just like an auto inspection report, a Net Risk audit can tell an underwriter more about the nature of an online risk than an application form. And in the case of large, multi-locational risks such as online banking operations, international distribution channels, or corporate intranets, an onsite audit should be mandatory.

Figure 4

4.6 Claims

Digital information can be manipulated. Firewall audit trails can be changed. To substantiate online break-ins and events, insurers must define specific steps insureds need to take to secure their audit trails. Net Risk provides insurers with some guidelines for securing evidentiary proof of claims in a digital environment, and further defines how IBM can assist insurers when investigating an Internet incident.

5. Insurance Opportunities and Exposures

Now that we have demonstrated how a secure Internet business operation can be built, its and assessed, its time to turn the picture and look at it from an insurer's perspective. Insurers provide a wide variety of products to businesses today. To see how these products need to be extended to cover Internet exposures, we need to step through each line of business and explore the online risks.

5.1 Crime insurance

Internet sits can be vulnerable to criminals and hackers. Websites, Intranets, Extranets, and electronic commerce sites are all at risk. Examples of unauthorized website penetration:

- Theft of information: credit card number, customer lists and account information, data-warehouse records, electronic cash, airplane tickets, stocks, bonds, insurance policies,

photographs, videos, music, and gift certificates are all examples of items of value that can be stolen in a digital environment.

- **Account manipulation:** bank account data, school records, government benefits, life insurance payments, pensions, and other account data can be manipulated with serious consequences.
- **Data stream monitoring:** Telephones can be tapped, cables monitored, even microwave transmissions can be intercepted.
- **Fraud:** Pyramid schemes, fraudulent electronic commerce sites, and non-delivery of service are already common Internet problems.
- **Denial of Service:** When websites are attacked and brought down, business interruption can result in loss of profit, and public image damage.

5.2 Internet directors & officers liability

Internet-related Lawsuits against the organization and the individual directors and officers of a company have already been brought to court. In Germany, the Bavarian government is suing the Directory of Compuserve for allowing Bavarian subscribers of Compuserve access to pornographic newsgroups in violation of Bavarian law. As most D&O policies do not exclude gross negligence, claims like this will be covered by existing policies. Other examples include:

- **Allegations of failure to provide proper protection of websites:** A hacked website might reveal valuable trade secrets, or financial data that could seriously damage a company and result in shareholder lawsuits.
- **Allegations of improper protection of websites:** Poorly implemented security can be as bad as no security. If a major department store Internet site is vandalized, public image may be damaged, resulting in lost share value. Shareholders may cry gross negligence and sue the Board of Directors.
- **Penetration to obtain “insider information”:** With billions of dollars at stake in large mergers and acquisitions, stolen or improperly disclosed insider information, obtained from a hacked website, could destroy deals and shareholder value, resulting in lawsuits.

5.3 Internet errors & omissions liability

Every company that provides website services will have to purchase Errors and Omissions coverage. With banks deploying Internet banking, Online book sellers making IPOs, and brokerage houses selling stock shares online, flaws in site design could cost millions and the designers may be sued to pay. Examples include:

- **Allegations of poor website design and development:** If a website developer designs a website that doesn't work, provides inaccurate or libelous information, the owner of the site may sue the designer for breach of contract.
- **Allegations of poor website performance:** If poor website performance causes an online brokerage house delays in derivative transactions, interest-rate swaps, options, or stock purchases, minor delays can cost millions. The vendor who installs the website faces third-party liability for that service.

- Claims against companies that service websites: Internet Service Providers face liability when their service downtime results in loss of profits for their subscribers. A good example is the recent out of court settlement between America Online and its subscribers resulting from 19 hours of downtime last year.
- Inability to access either websites or online services that provide access to the WWW.

5.4 Internet professional liability

Every webpage is advertising, unless specifically noted as containing editorial content. Therefore, every webpage carries advertising liability, and claims and lawsuits against Internet information publishers, content providers, PR agencies, advertisers, etc, can occur if the information provided is false, defamatory, libelous, or unauthorized. Examples include:

- Claims and lawsuits alleging false advertising, fraudulent information, improper use of websites: In the future, every link on a webpage must be authorized by the linked site. Businesses can be sued if they provide unauthorized links. For example, one can easily imagine church groups suing pornographic content publishers on the web for providing unauthorized links to their sites.
- Allegations of emotional injury caused by website information: Information online can be accessed instantaneously anywhere in the world. Libelous content can therefore be broadcast with global consequences. Even authorized website links placed in the wrong context can be subject to emotional injury suits.
- Allegations of defamation: "Flaming" is a popular term used in newsgroups to describe defamatory language used against another user. Newsgroups comprise editorial content that is protected as free speech in most countries. However, flaming on webpages is not protected by free speech unless it is specifically noted as editorial. Non-editorial flaming on websites can be subject to suits alleging defamation.
- Claims resulting from outdated, invalid, innacurate, or fraudulent information on a website: Webpages are advertising. Incomplete websites, outdated information, and innacurate statements can be brought to court as fraud. The Internet is an immediate medium, and information is assumed to be accurate and instant. Outdated airline ticket prices, hotel rental rates, changed business addresses, etc. are all examples of grounds for suit.

5.5 Internet workers compensation and product liability

Workers Compensation insurance insurers against workplace injuries. Workers can claim injuries resulting from online experiences or work, such as:

- Claims and lawsuits alleging defective design or manufacturing of internet products.
- Allegations of bodily injury or property damage as a result of accessing a Website because of the information contained in it.
- Allegations of bodily injury from using software has resulted in conditions such as repetitive stress injury.

5.6 *Internet property liability*

Claims to website owners or Internet Service Providers:

- Claims made for damage to websites or the assets that they contain or manage
- Goods ordered on the internet which are damaged, destroyed or lost in transit
- Business interruption as a result of the inability of customers to access a website because of physical loss or damage to the website.

5.7 *Catastrophic losses on the internet*

Fortunately, the Internet, designed by the US Defense Department to withstand nuclear war, is impervious to catastrophic loss. It can't be shut down or destroyed. But parts of it can be taken off-line, as was recently demonstrated by America Online (AOL), when its servers went down for 19 hours and its 3 million subscribers were left in the dark.

Currently, businesses and individuals access the Internet through Internet Service Providers (ISP). ISPs can be telephone companies, cable operators, online service providers such as Compuserve, Prodigy, or AOL, private networks such as the IBM Global Network, or government departments such as the US Department of Energy. Each one of these ISPs connects pools of servers to the public Internet backbone, and protects their servers with firewalls, secure gateways, and routers.

Since an ISP has the responsibility to provide service to a diverse group of companies and individuals, insurers should see ISPs as Special Risks. Special Risks need to be insured independently. Insuring the ISPs separately allows insurers to spread their risks according to size, geography, and Internet topology. This "Risk Spread" mimics the way insurers pool risks in the real world, and will, in a carefully managed risk portfolio, eliminate the threat of catastrophic losses.

5.8 *Managed risk*

If our merchant decides to build a real-world warehouse and house an Internet book store in the same location, she will have four implicit layers of insurance protection. The first layer will cover her physical location, equipment, and inventory against fire, damage, vandalism, and theft in a traditional P&C insurance policy. The second layer will cover her Internet location, the firewall, web-server, and inventory against damage, vandalism, or break-in. The third layer covers her Internet Service Provider against losses due to server downtime, hacker vandalism, etc. And the last layer covers her commercial transactions, deliveries, and communications encased in cryptolopes.

The combination of these four layers provides the merchant with a fully insured business. It also provides her insurer with multiple layers of risk protection. And the sum of the four layers make Internet risks fully manageable.

5.9 *Loss history*

In the real-world, Insurers base new lines of coverage on claims history. New claims over a period of time indicate new areas of exposure not anticipated in existing policies. Policy language is amended, excluding the identified exposure and new policies, or

amendatory endorsements, may be created to charge extra premium for the new exposure. Normally, this process allows insurers to calculate necessary premiums and reserve amounts using loss-rating formulas. In the real-world this process can mature over several years.

Figure 5

But the Internet is growing at over 100% each year, and it is totally un-insured. The rapid growth of electronic commerce means that businesses are creating new exposures that need to be understood in a proactive, rather than reactive mode. Insurers do not have the luxury to wait for claims to provide guidance.

5.10 Market size

The Internet is growing at over 100% each year. But an insurer that is selling auto insurance on the Internet might discover that only a small percentage of customers are even on the Internet. Even with 200% growth, it may take 5 to 10 years before all the real-world customers of an insurer sign up for Internet service. That makes selling traditional insurance on the Internet a frustrating experience.

But the market for Internet Insurance is the Internet, and the customers are already on the Internet. 50 million of them at last poll. So who could an insurance company sell Internet Insurance to?

They could start with their traditional commercial insurance portfolio and perform a census to determine how many of them have web-sites, intranets, etc. After mining that resource, they could turn to the customers of their competitors in their home market. And with the Internet totally unregulated today, any insurance company in the world could

underwrite Internet Insurance risks anywhere in the world. In short, the market is new, totally untapped, enormous, and growing very fast. For the first pioneers of this new insurance Line of Business, the opportunities are staggering.

6. IBM Solutions

As noted earlier, insurance underwriters, claims adjusters, risk managers, and administrators are largely uninformed about the Internet and unprepared to do Internet business. IBM can change that. IBM can help insurers get up to speed with the Internet today, stay on top of Internet developments, and manage Internet Insurance risks in the long term. To do so, IBM has prepared a 5-part service and solution offering. Top to bottom, this offering includes the following components:

Figure 6

6.1 Net risk boot camp

Before insurers can reap the benefits of online insurance, they have to grapple with the nuts and bolts of the Internet, Internet Security, and the threats posed by hackers. To prepare insurers for this brave new world, we have designed the following education curriculum.

Net Risk Boot Camp is a 2-day training course for insurance professionals – underwriters, claims adjusters, and risk managers – Internet Boot Camp is designed to introduce the insurers to the Internet from A to Z. Topics covered will include the origins of the Internet, risks and exposures, electronic commerce, legal issues, transactional and environmental Internet security, and an introduction to the Net Risk methodology.

6.2 Net risk exposure consulting

After the education, IBM will work with an insurer to help design Internet Insurance underwriting guidelines, claims report formats, product administration applications, and risk management seminars. In collaboration with ICG – using the IBM Net Risk Consulting Methodology – the Insurance ISU will help insurers lay the foundations for effective Internet Insurance risk management policies and insurance insurance products, taking into account issues of globalization, Internet marketing, and jurisdictional ramifications.

Matching the Net Risk exposure classification methodology to an insurers existing lines of business, IBM will provide a structured approach to Internet Insurance product development, encompassing the following areas:

6.2.1 Underwriting

Insurance applications need to be designed to map out potential perils and areas of Internet exposure. More than Internet hardware, software, and configuration, underwriters need to consider employee practices, password administration, and security policies and procedures. Guidelines need to be created to assess exposures, determine exclusionary wording to existing policies, and decide how to best craft new policy wording. Rate tables, deductible amounts, coverage limits, and discount practices will be analyzed using the Net Risk methodology.

6.2.2 Claims

Claims adjusters need to consider how to prove a claim on the Internet, secure evidentiary proof of incidents, how to file an Internet Insurance claim report, and what steps are needed to assess the damage and value of lost goods or downtime. Net Risk defines special measures insureds need to take to certify the integrity of their audit trails and incident reporting. These measures can be built into insurer claims processing guidelines.

6.2.3 Product administration

Administrators need to consider Internet payment collection, policy delivery, and claims compensation. Digital signatures, watermarking, and digital fingerprinting need to be evaluated for their effect on insurance policies.

6.2.4 Risk management

More than underwriting risks, insurers need to consider how to bring timely risk management advice to their insured to prevent losses. Insurers will need to keep up with the latest developments in Internet Security technology. IBM will assist by providing maintenance updates to the Net Risk intellectual asset, keeping insurers on the cutting edge of Internet development and Network Computing security.

6.3 Net risk audits and certification

Just like auto inspections, every website needs to be certified. The goal of the above service and solution offerings is to train insurers to be able to underwrite small and

medium sized risks. But no insurer today has the international presence necessary to underwrite Internet Insurance risk with global dimensions.

Banks, online department stores, and other mission-critical electronic commerce sites need a full scale Net Risk Audit. IBM can provide this audit and site certification based on the Net Risk methodology, on a local and global basis. To underwrite global risks, insurers need to outsource the risk assessment to a company with global reach. IBM can uniquely fulfill that need. In the future, IBM will certify business partners to perform these audits, providing insurers with choice in the delivery channel.

6.4 Net risk consulting services

Internet Security develops daily. To help insurers keep ahead of the development curve, IBM will provide quarterly updates of the Net Risk asset as part of a maintenance agreement. The updates will add industry-specific security exposures, hardware and software reviews, new hacker techniques, claims reports, and new policies and procedures.

6.5 Net risk claim audit services

IBM can help insurers validate the nature of an online incident and help assess the severity of the damage. Our Net Risk technicians can help insurance claims audit teams with technical expertise that can shed light on complex technical issues.

7. Conclusion

The conclusion to this White Paper is the message we have to deliver to the Insurance Industry. Bullets tell it best:

- **The Internet can be secured for commerce**
- **Net Risk can help insurers underwrite Internet exposures**
- **The market is large and exploding**
- **IBM can provide Internet Insurance Solutions Today!**

Insurers stand to gain a lot from this initiative. Access to new markets and new products top the list. But there is also the element of public prestige. Insurers entering this market will be identified as leaders in their industry, standard bearers for the others. And they will be seen by an appreciative business community as helping to make the Internet a safe and profitable arena in which to do business. They will be helping to make their name synonymous with secure Internet commerce.