

AMAX White Paper

“The Insuriti™ Zone”

*The New Solution for
Digital Risk Management*

January 2007

Where Insurance & Technology Connect

“The Insuriti™ Zone”

The New Solution for Digital Risk Management

©AMAX Consulting, LLC 2007
Legal Content Contributed by
Daniel J. Langin¹

Background: Cyber Crime and Data Security

Suggesting that cyber crime is a growing problem is a little like saying that the sky is blue. Theft of sensitive data has become so pervasive that the Washington Post dubbed 2005 “the year of the data breach².” Data thieves target companies that possess or exchange large amounts of sensitive data and then use this data to commit identity theft and related financial crimes.

Companies have responded by hardening the security of their internal enterprise networks and systems, but have not typically made similar investments to protect their data in transit. This has reduced security breaches that target network resources, but has made data in transit a more appealing target. Senior corporate executives and their companies’ Boards of Directors are now realizing that they have major personal exposures because there are no 100% secure hardware and software solutions that allow them to transfer risk. The 2006 CSI/FBI Survey indicates that last year the incidence of theft of proprietary information and unauthorized access to information remained at virtually the same level, despite the increased focus on improving security.

This is consistent with results from the 2006 E-Crime Watch Survey from CSO Magazine, which reported the average financial loss increased from \$507,000 in 2005 to \$740,000 in 2006. This survey also notes that targeted attacks are increasing, such as a 36% rise in theft of proprietary information (including customer records) and a 30% rise in intellectual property theft. Given that data eventually has to leave the network to go to external data centers, vendors and others, companies must find ways to reduce the risk associated with data in transit.

The Problem: The Business of Insuring Against Fear

The risks associated with securing data transmissions are found in the volume and the nature of data exchanged online. The last few years have witnessed an explosion in the amount of data transmitted online, especially sensitive information such as financial data, SSNs, human resources data, health data and trade secrets. Business models now dictate the need to exchange records online rather than via paper or removable media. It is simply more cost effective and faster in most cases to use electronic documents in the new “*Paperless Enterprise*.”

Growing Losses from Data Breaches

Because the volume and sensitivity of data in transit has drastically increased, it is no surprise that the **average loss** per data breach has also jumped. According to a survey by the Ponemon Institute³:

- more than 93,000,000 records of U.S. residents have been exposed since February of 2005
- the average cost of a data breach is now \$4.8 million
- the average cost to put new security measures in place after a breach is \$180,000.

¹ Principal of Daniel J. Langin, Attorney at Law, LLC. Dan has over 17 years of experience including thirteen years in technology, business law and intellectual property litigation and counseling. See www.langinlaw.com or contact Daniel at (913) 661-2430 or dlangin@langinlaw.com. This article is provided for educational and informational purposes, not as legal advice.

² “Ubiquitous Technology, Bad Practices Drive Up Data Theft,” *Washington Post* June 22, 2005.

³ Ponemon Institute, *2006 Cost of Data Breach Study*.

These figures may be too low--data losses are often underreported for fear of negative publicity⁴. The ones that *have* been reported are significant. BJ's Wholesale Club faced nearly \$13 million in claims and suits in 2005 from theft of data that BJ's failed to encrypt during transmissions containing personal financial information (PFI).

No Technology-Based Security Solution Is 100% Secure

There are multiple technology-based security systems in the marketplace today. They offer a variety of capabilities and security levels, and they continuously improve to try to keep pace with the growing threat of external and internal intrusions. However, none of these hardware and software solutions can guarantee 100% security or transfer the risk associated with potential losses. Digital certificates are useful for authenticating senders and recipients and for message integrity, but they do not secure the transmission process. SSL or VPNs are good for securing the transmission process, but they are not robust solutions for authenticating senders and recipients or data integrity. Furthermore, very few (if any) of the vendors offer to pay for data lost in transit, and if they do, payments are limited. The VeriSign NetSure Protection Plan, for example, involves a "per certificate lifetime" limit on a digital certificate (as low as \$1000) which applies to *all* messages or transactions that involve a certificate, whether one transaction or one million.

The Real Value of Lost Data

The real value of lost data, however, exceeds the cost to pay claims. The 2006 CSI/FBI study indicated that reporting of security incidents correlates **with a loss in companies' stock share value**⁵. The 2006 Ponemon Institute survey indicates that the \$4.8 million average cost of a breach (averaging \$182 per record) is made up of the following elements:

- \$54 per record in direct out of pocket costs (notification efforts, legal fees, PR efforts, etc.)
- \$30 per record in lost productivity (employee and contractor time)
- \$98 in lost business (both turnover of existing customers and difficulty in gaining new ones)

According to this survey, most of these costs were borne by Marketing (55%), Customer Support (34%) or Legal/Risk Management/Audit (11%) departments. Given that half of the cost of a data breach is lost business and such costs are not borne by IT, protecting data in transit is a **critical** business/risk management issue.

Who Pays for the Losses? What are the Real Consequences/Indirect Costs?

This breakdown of internal costs leads to an interesting question: Who pays for a loss of data in transit? Certainly not vendors. According to the 2006 Ponemon Institute survey product vendors are responsible for 30% of all data breaches but limit or disclaim liability in their service and license agreements. Insurers probably will not pay. The standard Commercial General Liability ("CGL") policy covers physical damage to tangible property, not loss of data.

⁴ See, for example, 2006 CSI/FBI Survey at 22 (figure 23) (most common reason that companies do not report incidents to law enforcement is negative publicity/loss of stock value).

⁵ See *id.* at 20, fn. 5.

Specialized technology policies offered by many carriers typically cover claims arising from a data loss or security breach of the insured’s network, but not a breach or theft of data in transit outside of the covered network unless caused by the insured’s own error or omission. Even then, the 2006 CSI/FBI Survey suggests that *only 29%* of companies purchase insurance to cover information security risks⁶.

Accordingly, data in transit often travels in a “no-man’s land” not covered by vendor contracts or insurance. This is the market opportunity for the Insuriti solutions. Insuriti™ is not an insurance product, but it creates both a secure method to send data in transit and a means to pay for its loss. Insuriti also provides processes for transferring digital risk.

The Security Gaps: Missing Components in Today’s Data Risk Management

Business reasons are not the only justifications for companies to protect data in transit. Companies need to plug gaps relating to compliance and organizational culture.

The Compliance Gap

Numerous laws, regulations and industry standards now require companies to protect sensitive data in transit. The graph below illustrates some of these requirements and the potential fines and penalties that can result from noncompliance:

Law, Regulation or Standard	Requirements Relating to Data In Transit	Who is Exposed	Fines, Penalties and Damages
Sarbanes-Oxley Act (SOX)	302 and 404 (internal controls over applications & systems affecting financial reporting)	Companies whose shares are traded on US public exchanges	Up to \$5 million in fines and 20 years prison time
PCI Credit Card Industry Data Security Standard (PCI)	Requirement 4 (safeguarding sensitive cardholder data during transmission over public networks)	All issuing banks and merchants/service providers that handle, transmit, store or process credit card holder information	Up to \$500,000 per incident
Gramm-Leach-Bliley Act (GLBA) and Regulations	Guidelines III.C.1.a (encryption of electronic customer information while in transit) and Safeguards Rule	All businesses that collect or maintain consumer financial information	FDIC can assess \$5,000 per day up to \$1 million per violation
Federal Trade Commission Act sec. 5A (FTC 5A)	Prohibits unfair/deceptive trade practices (including poor security for consumer data in transit)	All businesses engaged in interstate commerce	Largest yet is \$15 million (ChoicePoint)
Health Insurance Portability & Accountability Act (HIPAA)	164.312(e)(1) (technical security measures to protect electronic health information in transit)	Doctors and hospitals, payors (including employers with health plans) and health data processors	Up to 10 years in prison and \$250,000 fines

⁶ See id. at 10 (figure 11).

The Culture Gap

A prevailing organizational culture that focuses on security of data at rest increases the chance that a company will violate one or more of these laws, regulations and standards. This culture exists because companies tend to purchase solutions that are equipment-oriented and to ignore requirements concerning data in transit. A 2003 survey by Zix Corporation that sampled healthcare organization e-mail over a one-week period found that 4% -- *176,000 messages* -- contained unencrypted health information. Clearly many senior executives are not fully acknowledging the risk and are putting themselves, their companies, and their stakeholders at risk. With Insuriti, there is finally a solution.

Insuriti -- Patented Processes

Systems and methods for insuring data transmissions

Abstract:

Systems and methods are provided which afford a technical application for insuring, bonding, and underwriting a transmission of a data set, streaming data, and/or document over the Internet through TCP/IP and all other electronic media such as WAP (wireless application protocol), VOIP (voice-over IP), fiber optic channels, microwave channels, and through standard electrical switches, electrical outlets and power lines. The present invention includes a computer readable medium having computer executable instruction to cause a system perform a method for insuring, bonding, and/or underwriting data transmission. The method includes enabling a first remote client coupled to a communications network to insure, bond, and/or underwrite a transmission of an electronic data set, streaming data, and/or document, with a selected coverage type for a selected coverage amount, from the first remote client to one or more second remote clients. The method further includes charging a fee to an appropriate account for the selected coverage type and amount.

Perhaps this focus is understandable because data in transit is simply one point of exposure in the larger network risk management analysis, and it is easier to secure data at rest. As noted above, this point of exposure may become the preferred target of cyber-criminals as data at rest continues to be better protected. This makes the need for a solution to data in transit risks even more pressing.

Such a solution must set *de facto* industry standards, and include end-to-end tracking, indemnification and financial backing for losses. Organizations must be able to tag each transaction independently, classify types of data, turn unstructured data into structured data and apply risk mitigation to various levels. This hierarchical approach would enable organizations to manage the collection, storage, and transmission of data through the enforcement of standards, processes, procedures and policies.

The Insuriti™ Solution

A robust solution for the business and risk management problems affecting data in transit can be created based on patents for securing and bonding or insuring data in transit known as Insuriti. The elements of the Insuriti solution can solve a number of problems:

- Process management for enhanced information lifecycle management (ILM)
- An organization can classify different types of data, create structured data from unstructured data, and apply risk mitigation to the various levels
- E-document management
- Each transaction is unique and each transaction can be tagged independently
- Secured messaging system/IM
- E-Mail archiving requirements/audit trail
- Validated third party -- bondability and insurability demonstrate safety
- Not dependent on a particular technology platform
- Moves as fast as business -- digital version of overnight delivery, only faster & cheaper

Licensing these patents can help companies build solutions that meet compliance requirements and mitigate or transfer risk for data in transit. Licensees can pass on costs to customers or business partners and allow the license to pay for itself. It can also be used as a strategic differentiator and can even *save* money when compared to what a company pays annually for postage, overnight delivery and courier.

The processes covered by the patents include bonding, insuring and underwriting of Internet data transmissions.

Whether over the Internet, wireless connections or any other means, if data in transit is lost, a specific amount is paid to a designated party.

The Business Model

The holder of the Insuriti patents (described below) is prepared to make them available to companies that wish to develop processes to send and receive secure and bonded or insured data transmissions. The infrastructure requirements for utilization of the Insuriti patents are essentially technology neutral and can be tailored to fit each solution.

Managing the cultural shift will be part of the business model. In the same way that a prudent company would not in the past think of shipping goods without protection, it must now consider how to protect sensitive data (intellectual assets) in transit. Officers and directors are required to act as reasonably prudent persons to protect a company's interests, and many of the laws and regulations identified in this paper put compliance responsibility directly on a company's board of directors or C-level officers.

The Intellectual Property

U.S. Patent Number 6922720, entitled "Systems and methods for insuring data over the Internet" ("US1") was granted on July 26, 2005. U.S. Patent Number 7020692, entitled "Systems and methods for insuring data transmissions" ("US2") was granted on March 28, 2006. Copies of the patent are available from the U.S. Patent Office web site, www.uspto.gov. In a nutshell (and without limiting the scope of claims for these patents), US1 provides for the bonding of data transmissions and US2 provides for the insuring of data transmissions.

In addition to the current patents, several additional patent filings are in process. These include a U.S. patent for "underwriting methodology" related to bonded/insured transmissions. Patent recognition filings have been made in several foreign countries including the European Union and Canadian patent authorities. Based up the most recent updates, patent recognition in both the European Union and Canada is estimated to be granted in late 2007. A more complete update on these applications should be available in Q1 2007.

Unique Market Leadership Opportunity

The executive with vision will understand that the Insuriti patents offer a unique opportunity to become the market leader for securing and insuring data in transit. It also provides the opportunity to **control the market** through defining and establishing underwriting standards.

The Insuriti Zone: located at the intersection -- *Where Insurance & Technology Connect.*

For additional information on how Insuriti™ can work for your company, please contact:

Al Stern
AMAX Consulting, LLC
al.stern@amaxconsulting.com
612-743-9696