Operational Risks and the Emerging Social Contract
Implications to Asian Insurers

Gerald W. Hayden and Rachel Pong, Cisco Systems

Two of the most listed topics in business publications in the last couple of years have been Security and Operational Risk. The Operational Risks have largely dealt with the Balance sheet and Day-to-Day Operations. As more and more businesses are moving business processes such as Customer Self Service from the physical world to the virtual world of Networks, the Operational Risk are shifting with it.

Whether companies will be moving to a Converged Network where Voice, Video and Data share a common Network is no longer the question. The elimination of toll call charges and expense reductions for moving phone locations are examples of the **Productivity *Efficiencies*** a Converged Network can have. The new business processes, value propositions and business models which are being created have shown the **Financial *Effectiveness*** a Converged Network can have as well. The convergence of Efficiencies and Effectiveness is what a Converged Network does best, and serves as the foundation for Aligning Business Strategy and IT Investments.

The world is moving from an Economy of "Transactions in the Physical World", to one of "Interactions in the Virtual World". To provide a personal example of this transition, consider how many "conversations" you have with family members and friends in their physical presence, versus how many "interactions" now take place virtually via cell phone, text messages and email. Banks, Insurance Companies and Capital Firms continue to move more transactions and manual procedures to the Virtual World of Converged Networks. From an Actuaries view of the world, they would argue that by moving more and more business processes on a single Network, we are putting all our eggs into one basket. To use an insurance term, we are moving towards "Risk Density". The Actuaries argument would be theoretically correct. In reality, Converged Network Technology has been designed to mitigate this "Risk Density". In many ways it reduces Risk Density as it allows for real time monitoring of Business Operations through Video, Voice and Data Communications. The Risk lies in how well we integrate business process, people and the technology. How a Company architects, manages and operates their Network, is what many of the new Regulations focus on in regards to Operational Risk.

Foreign Regulation, particularly that being created in North America and Europe has created some significant challenges and opportunities for Financial Services Companies. Basel II, Sarbanes-Oxley and various Privacy Laws are beginning to establish the Global Standard of what a Company's Social Contract should be with its Policyholders and Investors. An example of this awareness by Executives is; in 2005 alone, 1 in 12 Financial Statements were restated. Although laws such as Sarbanes-Oxley only applies to Companies whose stock is listed on a U.S. Exchange, and Basel II only applies to Global Banks, they contain sound business management practices and their global affects have spread quickly. Some other examples of these include;

- Latin American Governments, seeing the wisdom of Basel II are virtually copying it into their Country's Regulations.
- One Mediterranean Country's Finance Ministry is using a Technology Consulting firm to assist in writing their Regulations regarding Operational Risk related to Technology.

- Chinese Banking will be required to "open their books" as a condition of joining the World Trade Organization.

Asian Insurers have the benefit of being able to view the experiences and shortfalls of others, but only if they recognize the potential affects Foreign Regulation may have over time. Even "Nationally" owned Insurers, who have longer term objectives of going Public, can take lessons so they can begin working on things today so they are in a position to compete effectively, and at their choosing.

Aside from the Social Contract issues, Regulators are continuing to learn more about the specifics of the Technologies and the associated Risks. Some of this learning is coming from accidentally finding a problem. Some of it is coming from a Company offering something they later wished they hadn't. And still others found documented concerns made by IT departments that Management didn't understand well enough to lead an effort towards correction.

Here are some trends we see on how Foreign Regulations will influence Asian Insurers over time and how it might impact their financial performance.

Protecting Our Investment Performance on the Balance Sheet

One of the impacts of legislation will be the need to adopt sound business practices that protects the Investments Insurers make. Insurance Investment Departments will begin asking, if Sarbanes-Oxley mandates a CEO can go to jail for inaccurate Financials, should I only "lend to", "invest in" or even "insure" a company who is Sarbanes Oxley Compliant?

Protecting Against Insurance Losses

Another factor of both Sarbanes Oxley and Basel II is based on the rules of protecting against Operational Risks. For example, In Basel II, Banks are asked to assess their Operational Risks and set aside Capital Reserves to cover for it. Theoretically, Actuarial Accounting says, if a Bank is Insuring itself against Operational Risk with Capital Reserves, any Business Continuity Insurance should be cheaper, and require its Insurer to hold less in Reserves. This is okay as long as the reduction in Insurance Reserves produces Returns that exceeds or equals the reduced Premium being charged. When this occurs the Insurer's margins remain unchanged or improve slightly. The point here is that just as Insurers spend millions in the "Physical World" training policyholders on things such as dangerous conditions in a work environment, or confirming the adequacy of their Fire Sprinkler System, they will be forced to acquire "new assessment knowledge" in order to understand the actuarial variables of "Virtual World" Risks. Insurers will become compliant through Actuarial necessity if they wish to continue to Underwrite Business Continuity Insurance. In the Physical World, it used to be the 100 year flood that would concern Insurers. In the "Virtual" world we now have to be concerned with things such as an email containing Malware that takes down the entire Network and stops business operations.

"Off The Book" Expenses

Recent emphasis by Regulators has been on defining "Off the Pro Forma Transactions". The thinking is Investors need to understand all the financial events of the Company so they can make informed decisions about the Stocks they invest in. Generally Accepted Accounting Standards has always advocated a conservative approach, and "Accrued" and "Reserve Accounts" are examples of how to handle these issues in an Accounting Sense. Converged Networks adds a new dimension to brick and mortar accounting. It was one thing when depreciation on a building

became fully amortized; everyone understood that "building maintenance expense accounts" represented the maintenance of the building so it would not fall down. As we shift to the Virtual World, the maintenance Risks are not so clear. CFO's and CIO's regularly hold off on needed IT equipment purchases to reduce expense to make the Profit Plan in lean years. In the virtual world this can be the equivalent of not repairing a broken lock on a Cash Vault door. CFO's and the Regulators are beginning to understand they need to begin thinking about how we Account for this type of "end of equipment life" risk. How does one account for expenses which you should have made but didn't is the question, other then reflecting the Risk in Reserves. One major U.S. Bank was recently asked to respond in writing to a Regulator's question, "What are your provisioning and de-provisioning plans for your technology". This trend is important and suggests an emerging understanding of the shift of business process from the physical world to the virtual one, and the inherent Risk which follows this transition.

As we mentioned before, Insurers need to ask if the companies they are investing in are Sarbanes Oxley Compliant. This includes both the accuracy of their financial statements as well as the management of their Operational Risk. If the answer to these questions is not known, consideration should be given on how much market capitalization might be lost in the event of a prolonged outage, or a network breech which leads to Policyholder Identity Theft. The trend by U.S. Regulators is to fine violators based on trying to cover Investor losses. Although it appears much of the Fines are not actually making it back to Investors, the fines have none-the-lessbeen significant based on this thinking.

In Basel II, for Banking, the Operational Risk component is fairly clear. Define Risk, and place Capital Reserves aside to cover it. There are some Financial and Risk alternatives:

- Transfer the Risk by buying Insurance. Unfortunately this may not work as well when it comes to Privacy Law violations. For example, you can purchase insurance for Policyholders so that if someone penetrates the Network and steals their identities, insurance will cover the legal fees and other costs to restore the Policyholders Credit Rating. In the U.S., prices can be as high as $6 per customer and it can become very expensive over a large customer base. However, this insurance expense does not eliminate the Regulatory fine that would also occur.
- Make the technology investments in the Network to mitigate Network Penetrations, as identity theft insurance only solves part of the problem. The advantage of the technology solution is that Privacy Laws requires that customers who may have been affected, need to be informed that they are at potential risk. The notification must also be timely. This is largely becoming the first choice as companies consider the penalties being assessed, the need to have to do it anyway, and it will eliminate the Fines. It also provides a foundation to re-engineer business processes that enhances Financial Performance of the company. Conservative thinking would say, if I have to make the investments anyway, I might as will make sure it pays back. One Executive furthers this thinking by saying, "those who implement technology only to meet regulatory need and mitigate risk, does not understand that any investment, no matter what the reason, needs to financially perform and that is the role of the Business Side, not IT"
- We need to consider the consequences of doing nothing, and continuing to assume the Risk. Management in a Country with limited or no Consumer Privacy Law can take the position, we will do nothing and assume the Risk, because there are no financial penalties, and no affect on our Balance Sheet. The problem with this thinking is once a large part of the world adopts one method

and makes clear the socially responsible contract they wish to have with their Policyholders, it forces others to reach the same standard, except in record time. If they have to pursue a record time approach, it can double the IT investment required as provisioning costs typically can not be handled with existing technical staff. This can also introduce other expenses to general business operations such as Overtime Pay caused by Network Outages. Approximately 20% of these outages will be due to the Skill set deficiencies of the Network Systems Engineers whose learning was delayed by an unplanned approach.

- One interpretation of Sarbanes-Oxley requires that companies have provisioning and de-provisioning plans for their equipment. The days of holding onto equipment well beyond its "end of life" is quickly becoming a thing of the past. It may be okay with Printers, but not for Network Equipment that controls Access to the Insurers Network. Insurers risk their reputations of "Public Trust" if they fail to meet this business practice standard. Even if a Network breech only causes a 1% impact to their Stock Price, how many millions of dollars might this represent to Shareholders?
- The relationship between the Insurer and its Policyholders is one of significant Trust. Policyholders by the very nature of Insurance is entrusting the Insurer with the safety and welfare of their families, property, employees and businesses. Should an Insurer protect this trust and what might happen if this trust is broken?

Shift from Physical Insurance to Virtual Insurance and a New Revenue Source

The key variable in minimizing future Losses and making Safer Investments assumes Insurers understand how to underwrite all of this. Whether we guess wrong on the Reserves or the Premium amount has similar long term affect. Understanding these new variables will take time, and claims will improve the underwriting as it has always done. However, there will be one difference between physical insurance and virtual insurance and that is the intellectual capital source Insurers will be depending on over time. Underwriting and Actuarial Accounting will play a large role, but where the Insurer learns from may very well be from their Network IT Department. Creating new Business Continuity Insurance Products and getting Policyholders to an "*Insurable Network*" could provide significant differentiation and new Revenue streams for those Insurers with the Vision to see it, and with the experience that will allow them to underwrite it profitably.

Conclusions and some Possible Actions

Asian Insurance Executives may want to come to conclusions about their Social Contract approach sooner then later. Those who aim at "nothing" will hit it with amazing accuracy. Consider some of the hard lessons learned by those Corporations who have run up against the Regulations in the U.S. and Europe.

1. ***Manage Risk and Don't Gamble*** - A Converged Network typically takes 2-3 years to deploy. It's not something that can be easily fixed halfway through deployment, as the added cost for fixes and re-provisioning can almost double the overall costs. In effect, we may be avoiding 1-2 years of Capital Charges, but risk doubling the overall cost if something happens. An Actuary might ask, is this sound Risk Management or Gambling?
2. ***Risk Management Policy should Align with Policyholder and Shareholder needs*** – To do nothing means assuming Risks "off the balance sheet", and hope the 100 year flood does not occur. If something does occur, there are no Reserves to insulate Financial Performance to the detriment of Policyholders and Investors. By default, this means Management's direction has been in

direct conflict with Shareholder needs, and they have chosen to ignore a fundamental financial practice of insurance called "Reserves".

3. ***Determine where you are today, and where you want to get to*** – A Converged Network will be the foundation of future Insurance Companies as they continue to migrate their business processes to the virtual world. One thing that is clear from the experiences of others; The first thing a Company does after paying a large fine, is to pay for the required technologies to protect against reoccurrence. This means they pay for what they could have done in the first place, plus an additional a premium in the way of fines. The cost of this risk is basically the cost of the possible fine, and typically matches or exceeds the amount of the investment that could have been made to mitigate it to begin with. The difference is the "fine we are forced to invest in" has no hope for financial return.
4. ***Operational Risk is a Business Issue not an IT One*** – More then one CIO has made the mistake of thinking Operational Risk in the way of Security and Operations is an IT issue. It is incumbent upon them to view the costs of assuming the risks, the off-the-book costs, employee overtime, the additional servicing costs, provisioning costs, lost Policyholder Trust, Loss of Market Capitalization and the potential for fines, and articulate these to management. As one CIO put it, "at least when I put these issues in front of management, they can't say they didn't know". One thing the regulators have been clear on when they have found violations; the size of the fine is partly determined by how proactive the Company was in their attempts to manage to Operational Risk to begin with. Since it typically takes companies 2-3 years to manage to this Risk in the way of their IT Investments, Management needs to give thought as to when they should begin.

Summary

Much of the new regulation is really fine tuning past thinking of making sure there are adequate Capital and/or Reserves to cover Balance Sheet and Operational Risks. An increasing emphasis is being placed on Operational Risk. Regulators are beginning to understand the Physical to Virtual World Operational Risk transfer. As Insurers continue to shift Business Processes and Transactions from the physical world of Headquarters and Agent Offices to the Network, new risks emerge. Insurers have understood the probability factors of 100 year floods, and the safety factors to protect against fires, and built these into their Actuarial Tables, Underwriting, Reinsurance and Reserves. Now a new "Virtual" threat is being introduced. Time and space are disappearing and now a 15 year old prodigy from another Continent can threaten their business operations from thousands of miles away.

Although many Asian Insurers may not be legally bound by these types of Laws today, the intent of the Laws and the concepts of managing Risk make good business sense. Since the Network plays a larger role in Operational Risk going forward it may make sense to gain expertise in the deployment and management of Converged Networks as quickly as possible. Whether Insurers chose to be proactive in Operational Risk Management or not - there will be a price to be paid. Whether we increase Reserves or make the IT Investments is not the simple choice it used to be. The advantages and benefits of a Converged Network will far exceed the costs of meeting regulatory need and allow Insurers to go well beyond their future Social Contract.

Gerald W. Hayden
Cisco Systems, Incorporated
New York, NY, USA

Rachel Pong
Cisco Systems
Hong Kong SAR, China