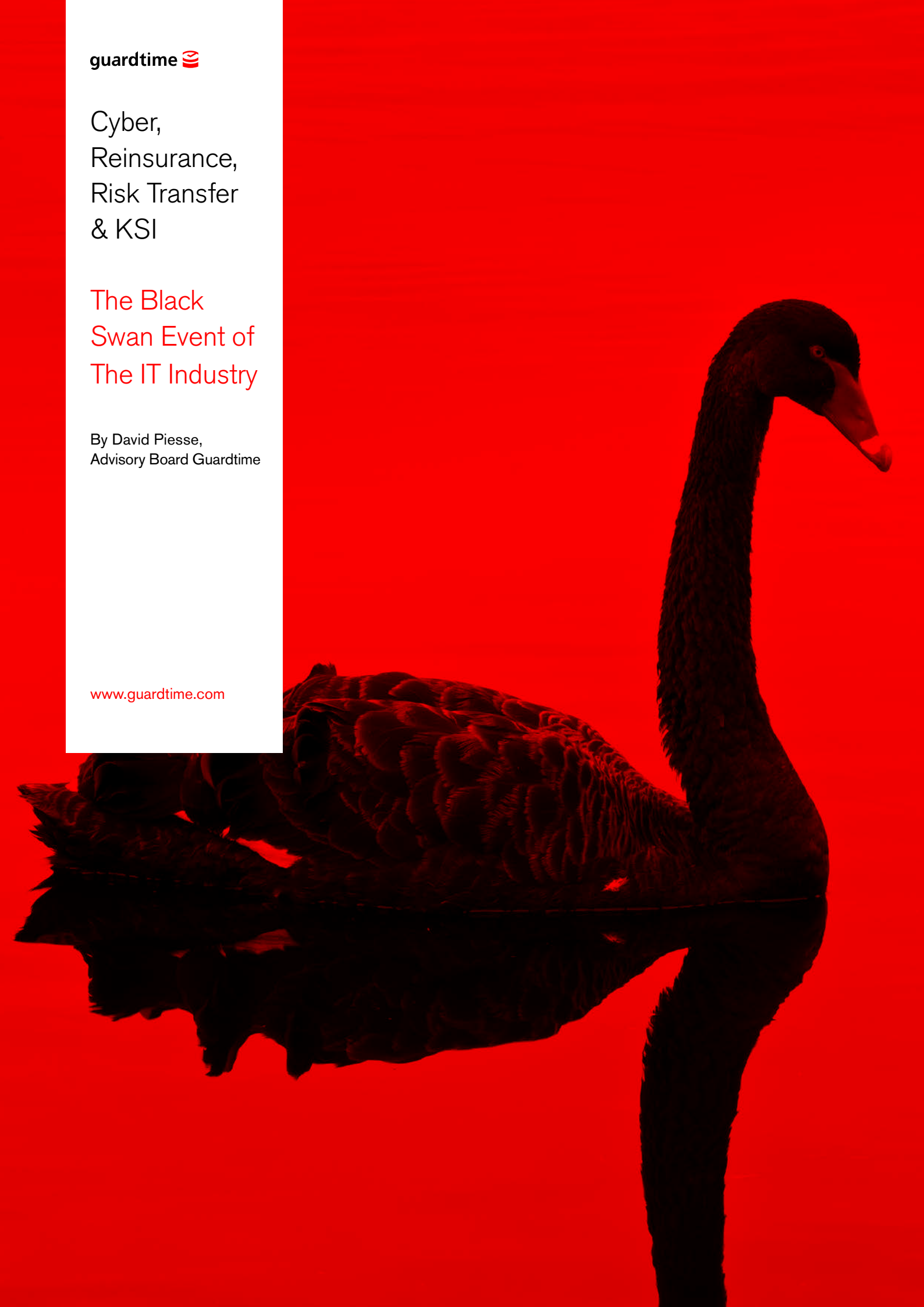
guardtime

Cyber, Reinsurance, Risk Transfer & KSI

The Black Swan Event of The IT Industry

By David Piesse,
Advisory Board Guardtime

www.guardtime.com



Overview

The reinsurance industry is known as the secondary insurance market as it provides insurance cover and risk transfer to insurers and is not seen by the public. However it is the stability mechanism for solvency in the insurance industry and the link to the capital markets and pension funds that are used to fuel calculated risk based investments.

The reinsurance industry is facing an emerging technology threat in the form of cyber risk. This is part and parcel of the transformation of how business is conducted globally where people interact via smart phones to the commercial Internet and social media. This means that technology has redrawn the boundaries of modern society. The reinsurance and insurance industry must protect this new world of machine to machine interaction (M2M) in the future the same way that it protected the old and status quo for the last 300 years.

This means introducing new technologies and standards to provide warranty and risk mitigation against cyber risk and data breach. The purpose of this paper is to introduce KSI (Keyless Signature Infrastructure) to the reinsurance industry as that standard for the purpose of cyber security to all governments and corporations whether large or small. KSI will help the industry metricate and model the cyber risk correlated with other risks thus including cyber risk in the solvency, risk based capital arena with fat tail exposure reduction.

It is very easy for organizations to be reactive to cyber events and say “it will never happen to us” and then when the event does happen it is costly in both financial and reputational terms. This can directly affect the solvency of the organization by loss of customers and can result in a country rating downgrade for a nation.

It is difficult for governments to determine if a cyber attack on a company is an attack on that company or the start of a cyber attack on a country as happened in Estonia in 2007 where the whole country was cyber attacked. This means governments now want to know the extent and nature of the data breach especially when IP theft of loss of private data of citizens is involved. The mechanism being introduced to do this is a mandatory data breach law or strict guidelines which forces organizations to report data breaches within a specified period of time or face heavy fines up to 10% of gross annual income for failure to comply plus the reputational risk which may takes years to recover. Ignorance of a data breach having occurred is not an acceptable excuse and will receive the same penalties. Such laws and guidelines are already in USA, just starting in Australia, being reformed in the EU over the next year and various stages of development in the rest of the world. This fine against annual income will be ROI (Return On Investment) to adopt and invest heavily into risk mitigating technologies, standards and best practices closely related to risk assessment and enterprise risk management such as KSI.

Cyber risk comes about because of the use of technology in the handling of all data and related information. Data is the greatest asset of any organization. Cloud computing is undoubtedly a positive evolution in all organizations as it reduces IT costs, reduces carbon emissions from data centres and provides a faster way of doing data analytics across multiple processors in a short space of time. This is essential as solvency, catastrophe and risk models mature they will be used more and more by boards of directors for daily risk decision making.

As the data volume is so large cloud power is requiring to deliver the outputs at the required time. Akin to the benefits of cloud computing comes government regulatory fear of data being tampered on the journey in the cloud causing data breach in a market place where all stakeholders and players become insiders thereby increasing the risk of fraud and data tampering. These multiple cyber threats stem directly from social engineering which has created a new underground criminal industry that trades on IP theft and stolen data.

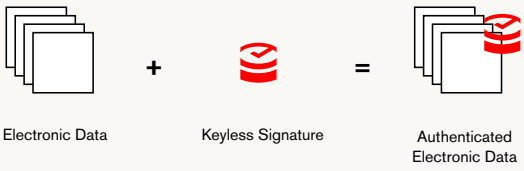
The response to this threat is an aggressive and proactive regulatory environment to create standards and best practices. Daily case studies are seen in the media showing the rise of cyber attacks globally.

To date the reinsurance industry has really followed the insurer in looking at what the risk means and how can the risk be transferred using the existing mechanisms of the risk industry i.e. reinsurance, captives, catastrophe bonds, sidecars and other special purpose vehicles. As up to 30 insurers now write some form of cyber insurance coverage outside of E&O embedded risk (Errors and Omissions insurance) the reinsurance industry needs to look at the effect of large aggregated cyber attacks which can really affect the capital and stability of the risk industry. These are black swan events and a parallel can be drawn from physical event damage such as earthquake and flood, reputational risk in global financial market meltdowns, healthcare pandemics to digital data damage caused by large cyber events. This means the reinsurance industry needs to understand cyber risk independently of the insurer so they create the right protection mechanisms. This will mean evolving cyber models and rating bands. The next section introduces KSI technology.

KSI Standard and Reinsurance

KSI (Keyless Signature Infrastructure) addresses the notification of a data breach which is essentially a peril with the intent to copy, extract or destroy data. This peril alone can give rise to a multi peril situation including cyber extortion, cyber terrorism, recovery costs, loss of revenue, reputational damage and contingent business interruption and supply chain disruption. One only has to look at the Thailand floods of 2011 to see the damage supply chain disruption can impose and wreak havoc in the globalized world. Again this is the parallel in the digital world. Organisations and risk buyers will expect insurance cover organized by their insurance brokers and subsequently the reinsurance brokers to cover the insurers.

KSI can be thought of as a “lie detector for data”, a simple process of signing a piece of data by software whether it is a policy, claim, reinsurance transaction, PDF document, email or analytical data.



Data signing can also be imbedded in devices producing documents or files such as medical equipment, printers and map-making operations. KSI provides keyless signatures to deliver proof of signing authority, signing time and data integrity. Verification is based solely on mathematics and does not rely on a trusted third party or the security of cryptographic keys. Thus for organizations there is no need to worry about being compromised by counterparty risk. This provides data assurance and immutability on the attributable Internet.

KSI will be the necessary component in this equation to guarantee the notification of a data breach as an official standard process. It will not prevent hacking from insiders but it will stop hackers from covering their tracks. This can be illustrated nicely in the case studies of where large amounts of documents or data are removed without knowledge of the organization. If the IT (Information Technology) logs are signed by KSI early notification would prevent or greatly minimize an undisclosed theft of large volumes of data. In a similar fashion banks would sign the ATM logs with KSI to provide non repudiation of events at the ATM and thus protect their reputational risk.

KSI would exist in the risk assessment questions of the reinsurance brokers and in the policy wordings of the cyber liability policy leadings to warranties and discounts of premiums. This will give reinsurers the confidence to offer capacity (capital) to the insurers so the risk can be properly handled and managed. In turn this will lead to reinsurers being able to quantify and model the risk for reinsurance optimization and cyber risk capital pricing thus correlating the risk with other perils such as natural catastrophe, market risk and credit risk.

For reinsurers to get independence in cyber risk management they will need to get the frequency and severity of cyber attacks for historical events and have access to a rating system of IT vendors on the quality of data and their mitigation of data breach threats which also involves the use of KSI at the vendor and outsourcing level.

For the insurance industry KSI will greatly increase the uptake of cyber liability policies while at the time reduce data breach expenses which in turn leads to reduced legal reserving, reducing combined ratio and increasing profitability of the risk and lines of business. Lets take small window into supply chain risk and cyberspace events.

Supply Chain Risk

Recent natural catastrophe events have shown what can happen to the global supply chain in terms of disruption especially in emerging nations where large industrial parks were built in catastrophe prone areas and developed quickly in order to compete with developed nations. Little thought went into risk management and mitigation. Referring again to the Thailand floods this particular event brought an unprecedented insurance and economic loss causing contingent business interruption to the world's car and hard disk manufacturing markets.

A severe cyber attack would have a similar effect on the global supply chain especially around the commercial and industrial Internet usage. Loss and tampering of data affects an organisation's ability to conduct business , disrupts other business contingently related and seriously impacts reputation and associated costs of remediation , litigation and notification around compliance leading to fines and solvency issues. Again enter KSI in the supply chain risk mitigation.

The insurance industry knows that the outsource service provider is the main cause of supply chain disruption and often happens at the same time as increasing weather disruption bring in the two large emerging risk of cyber and climate together in one event. Technology existing in conjunction with cyber attacks and service providers make up the majority of all the supply chain disruptions. When outsource service providers outsource to each other this a red alert to the insurance industry. KSI needs to be imbedded both sides of the equation in the enterprise itself and in the IT vendors they outsource to and to the vendors those outsourcers in turn engage. Only this way can there be an effective subrogation process based on non repudiation to recover and share fairly the claims incurred from a data breach. So now it is key to look at how companies might look to risk transfer their cyber risk today and then later in the future.

Cyber Captives

Captive insurance is a risk transfer tool of enhanced risk management, reduction of the cost of risk and often tax benefits. It is particularly well suited to cyber risks. More than 80% of FORTUNE 500 companies benefit from captive insurance and as this is a well trodden path need to extend it to cyber. A cyber captive is an insurance company attached to a parent insurer or group specifically designed to handle the cyber risk of the company. More companies will use cyber captives to help address the ongoing risk of cyber attack. Some will be a cyber only captive and others alongside other special risks such as earthquake. Another advantage of the cyber captive is the occurrence based policy wording, protected by KSI, which applies to data breaches occurring during the policy period given a longer timeline for claim reporting and payment allowing for a build-up of essential captive claim reserves. These cyber captives can then be used to access the larger reinsurance market for capacity.

Cyber risk that attracts the reinsurance industry is *high severity* and *low frequency* as the insurance industry can handle the small occurrences unless they are aggregated into a bigger event by some other event. This is the reverse of other captives which were based on *low severity* and *high frequency* where a large number of claims resulted in lower capitalization costs in handling the claims. However many risk buyers and risk managers are now discussing with their brokers about the option of using captives for the cyberspace so they can tailor this risk for their organization and not go to the open market for insurance. Data breaches are an expensive risk and the captive can underwrite and pay claims from a cyber reserve thus relieving the parent company of multiple risks and reputational issues. KSI would need to be part of the captive risk management. However there is no risk transfer without data and risk models. In order to model the entry point and economics of a captive and other risk transfer mechanisms we need to have access to sound historical data.

Cyber Catastrophe Models

Internal resources have to be deployed to handle a cyber crisis and these services can be offered by the insurers as part of the cyber liability cover. Large databases are being developed to access the frequency and severity of attacks containing recent breaches on a global basis and recording the associated costs of handling the breach. These event models or cyber cat models can be used to help create cyber XL rates (Excess of Loss) for reinsurance cover and move away from quota share reinsurance which is only required in the early days of reinsuring a new risk.

These cyber cat models will mature the cyber reinsurance industry the same way as they did the natural catastrophe lines of business. These databases would also need to include legal expenses as these are particularly perilous to solvency and to the proper reserving of claims (the ability to pay) over a particular period of time. Like all the perils before cyberspace risk will be subject to regulation and rating which will force the entities down the path of Enterprise Risk Management if they have not already done so and this will be the defining force moving forwards.


PHONE
PHONE

Regulation and Rating

There is no doubt of the increasing regulation in data breach reporting that will lead to increased cyber liability cover end even mandatory insurance in some cases. Within this emerging global regulatory framework sits the issue of rating both at the sovereign and corporate level. Rating agencies can have an economic effect on countries and corporations by making changes in rating as a result of an economic event. The rating of insurers is also at risk if they do not provide mitigation advice to customers as if a rating drops to certain level then they will not be able to get reinsurance capacity and thus become more exposed to the risk. Similarly reinsurance rating downgrades can restrict access to "A" rated capital meaning the likelihood of default on claims could occur. It is in everybody's interest in the regulatory and rating space to understand the standards and value that KSI brings to the table.

Rating is a science to measure the effectiveness of companies and countries based on their risk management approach. Currently the rating agency world has not been able to address the cyber space as the insurance industry has not been in a position to measure cyber risk liability. Rating agencies will view cyber as a primary threat to solvency because of the significant, rapid and unexpected impact of an event and it some cases the ability to react to that event.

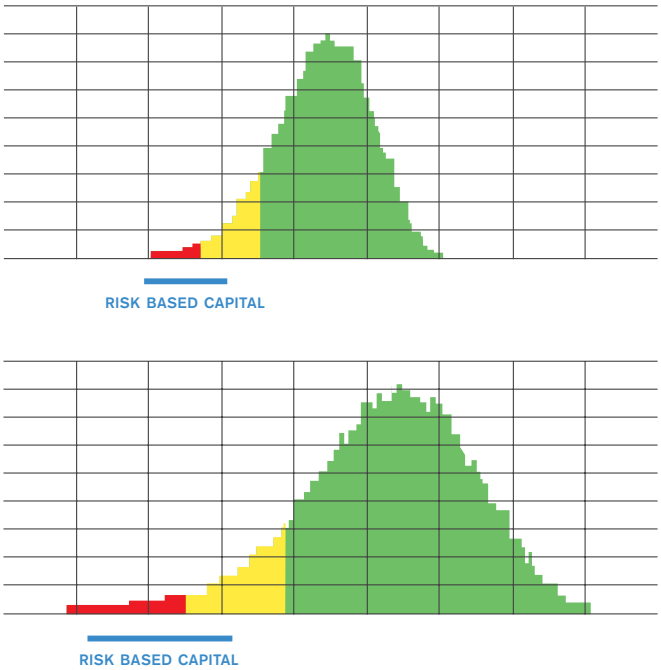
In the natural catastrophe world rating agencies look at the use of catastrophe event models that are created by third party vendors and they rely on the accuracy and research that has been done by the vendors on the data. Sometimes these models are blended to get an average view. However in the case of cyber the catastrophe is the data itself so that means there needs to be a broader rating approach i.e. that of data quality and the IT companies and outsourcers that handle that data. This means a data scoring rating mechanism is required that can be added to the risk assessments for global rating agencies when they measure the effectiveness of the enterprise risk management of the entity they are rating. This means that corporations can take the output of these newly emerging data rating agencies and make comparisons in their internal risk models of the various third parties being used and make better risk mitigating decisions while insurers can make better technical underwriting decisions. The companies using KSI will receive a higher rating as they have mitigation in place in line with international standards and best practice. We will cover Enterprise Risk Management in more detail.

Enterprise Risk Management

Companies manage many risk aligned to their risk profile and risk appetite all dependent on the industry sector. They do so by risk awareness and risk assessment and the visionaries and early adopters in the industry do so dynamically by use of mathematics (stochastically or actuarially) using simulations for the future based on the historical loss data in order to correlate all the risks of the enterprise into one holistic view. Operational risk affects every organization on an equal opportunity basis and is very hard to quantify and is often just quoted as a % of gross written premium. Cyber should be no different in terms of any other risk in terms of risk management and risk transfer. IT departments even with the best of intentions can increase the cyber risk by their policies and there is no solver bullet to protect the company. KSI does enable companies to plan data breach strategies where systems administrators are no longer involved in the security process which will bring great comfort to risk managers who see a lot of new technology being introduced which increases the cyber risk even with best intentions.

Insurance and reinsurance are not an alternative to an enterprise risk management program. Risk transfer programs should be used to address structural residual risk which means companies can identify the risk and then adopt risk management best practices like KSI to ease the process of finding the right cover at the right price with the correct reinsurance optimization which also includes tailoring the risk into the cyber captive as already covered. When the policy wording indicates the use of KSI this would not be KSI protecting a few documents or emails but KSI plugged nto every facet of the enterprise as a complete software appliance. The insurance industry should insist upon this enterprise level of risk mitigation before they issue cover for the large risks and data breaches.

The following diagram shows a risk modeling exercise using a robust industrial risk modeling tool looking at cyber risk. The green portion represents all the small claims that could result from a cyber attack based on historical data available and within the guidelines of the risk appetite of the concerned entity. The yellow portion shows the move to riskier areas and the red portion is the fat tail or the black swan event that could make the entity insolvent. This is the tail value at risk (TVAR) and the area that needs to be risk mitigated by risk transfer mechanisms of which the obvious one is reinsurance. However as we have established that reinsurance in not the replacement for best practice risk management we will make an assumption that KSI has already been adopted here so we are looking at the residual risk mitigation following KSI implementation. The bottom graph shows the situation prior to reinsurance where the small claims are aggregated and a long fat tail cutting into the companies risk based capital limits. The top graph show a leaner risk situation after the application of reinsurance bringing it back in the comfort zone. The standard deviation process will also depend on regulatory standards of how the regulator views cyber risk and solvency. Currently solvency models are geared on average to a 1:200 year event which may be suitable for earthquake and other peril risk but likely to be different for cyber and will vary by country risk appetite.



Following on from reinsurance we can look at other risk transfer mechanisms. Cyber captives have already been mentioned and a point worth noting is the potential to mathematically create a “cyber index” in the same manner that weather indexes and stock market indices appear in the macroeconomic models representing market risk exposure correlation to other enterprise risks. This cyber index could be created from the data patterns of the cyber catastrophe models and other data and then used as a threshold to trigger a data breach claims process following notification of a data breach by KSI.

The other environment is to move to a special purpose vehicle (SPV) risk transfer approach in conjunction with capital market investors and sponsors. This would be similar to the catastrophe bond investments that protect countries from earthquake risk by creating a bond shared by government and private industry to pay and share claims by loss bands in the event of a large or lack swan event. These public:private partnerships exist and are very effective and can be applied to cyber. However such bonds often have a 10 year span and a shorter life span vehicle will be more suitable to cyber. For natural catastrophes these 2 year vehicles have been referred to as sidecars which is a SPV derivative of a captive where investors invest in a risk via “A” rated hedge funds and then after the event has not taken place in a time frame receive their money back with interest. This makes cyber risk then part of an uncorrelated portfolio investment for the Chief Investment Officers. They can also base investment on the severity level of the attack so investments are not lost on all events. It will take time for this SPV approach to evolve over reinsurance and captives but with good data quality, proper event models, proper ratings and adoption of KSI and other standards in the IT space the capability to use capital markets to risk transfer cyber risks will emerge. KSI would give investor confidence in such SPV’s.

Conclusions

Large brokers have identified cyber as an "*equal opportunity risk*" and made statements like "*Acts of God are becoming acts of man*". No one escapes the cyber risk which is not a niche. It is now number 3 in the risk table of the industry following only taxation and loss of customer. Being proactive and recognizing the need for cover has been led to date by the USA and is spreading to Europe/ MENA and soon to the multi-cultures of Asia Pacific and South America. New and fresh cyber events causing disruption can accelerate laws in countries not yet developing their data laws. KSI will allow companies to do proactive risk analytics on a day to day basis binding this best practice to other risk mitigating services. Soon we will see a vibrant global cyber insurance market with a highly supportive reinsurance sector for the larger risks backed by the capital markets and sponsors who understand the risk.

Risk management of a data breach must be built into company policy at the board level and need to be non reliant on IT Departments which can be achieved by the use of KSI. Brokers need to know the details and customers need to see the bigger picture. We can use the benefits of KSI in the industry to help brokers understand the risk and ensuing policies. , help insurers with their services for data breaches and customers to understand the facts of the risk.

KSI will give the reinsurance industry the confidence to provide reinsurance capacity to insurers as they will have a quantification of the risk. In the same way it will give the capital markets the confidence to drawdown capacity to reinsurers to cover cyber risks and lastly the confidence to investors to place part of their portfolio in the cyber SPV and catastrophe bond space.

KSI will give the regulators and rating agencies the confidence that Enterprise Risk Management has been included in cyber liability cover and managing consultancies will have benchmarks to forensics.

A global outage of the Internet, like a meteorite attack, will likely never be covered by cyber liability insurance, but KSI will provide risk mitigation and opportunity for the business world to continue their practices protected in the wired and connected world the same way as they were in the past.

guardtime