Mitigating cyber risk for insurers
# Contents

3  
Executive summary

5  
Enterprise risk management correlated to cyber risks

9  
Security issues affecting reinsurers

11  
Supply chain risk

13  
Cyber captives and risk transfer

15  
Cyber liability regulation and rating

16  
Leading practices and the Center of Excellence

17  
The future intangible world

17  
How EY assists with effective cyber risk management
Cyber security threats are one of the most important risks facing the insurance industry, yet other industries are ahead in monitoring and managing them.
This is the second in our two-part series on cyber security that highlights the data and risk issues that are so prevalent today in the world of information security. Both papers offer a broad view of why this topic is so important for insurance companies and how they can protect their businesses from rapidly emerging threats.

This discussion explores the risk aspects of cyber liability insurance and looks at how insurers and reinsurers provide warranties and mitigation as part of their risk assessments. Our first paper on cyber liability insurance1 focused on the three pillars of information security: confidentiality, availability and data integrity.

In the last decade, actuaries have used new technologies and high-speed computers to analyze data at speeds unimaginable before. Catastrophe exposures, longer life spans and health care increase the need for modeling and analytics, as do the new emerging risks stemming from computing, climate change, asset bubbles and nanotechnology. The data used for risk-based pricing, however, is still coarsely grained at the customer or policyholder level. It may be perceived that risk is being shared equally, but in fact, the risk profiles are very different when analyzed – which goes to the heart of risk pooling and the concept of the industry itself.

Key contacts:

Shaun Crawford
Global Insurance Leader
scrawford2@uk.ey.com

David Piesse
International Insurance Society (IIS) Ambassador for Asia Pacific and Insurance Lead at Guardtime
david.piesse@guardtime.com

Insurance is a risk industry that analyzes good data in order to evaluate, comprehend and mitigate the risks.
Enterprise risk management correlated to cyber risks

The advent of new technologies has enabled risk stakeholders to perform enhanced data analytics to gain more insights into the customer, risk assessment, financial risk management and quantification of operational risk.

Companies manage many risks aligned to their risk profile and risk appetite. They do so by risk awareness and risk assessment. The visionaries and early adopters do so dynamically by use of mathematics (stochastically or actuarially) and simulations for the future based on the historical loss data in order to correlate all the risks of the enterprise into one holistic view. Factors to consider include:

**Cyber risk.** Operational risk affects every organization on an equal basis and is often quantified as a percentage of gross written premiums. Cyber risks are no different from any other risk in terms of risk management and risk transfer. However, IT departments, even with the best of intentions, can increase cyber risk by their strategy — and there is no silver bullet to protect the company. Keyless signature infrastructure (KSI™) enables companies to plan data breach strategies where systems administrators are no longer involved in the security process. This will bring great comfort to risk managers who see new technology being introduced that will increase cyber risk.

**Risk mitigation.** Insurance and reinsurance are not alternatives to enterprise risk management (ERM). Risk transfer programs should be used to address structural residual risk. From EY’s experience, companies can identify risks and adopt risk management leading practices to ease the process of finding the right cover at the right price — with the correct reinsurance optimization. The insurance industry should insist upon this enterprise level of risk mitigation before it issues cover for large risks and data breaches.

**Risk modeling.** The exercise in Figure 1 uses a robust industrial risk modeling tool to look at cyber risk.

The red is the tail value at risk (TVAR) and the area that needs to be mitigated by risk transfer mechanisms. Reinsurance, the most obvious mechanism, is not the replacement for leading-practice risk management. The assumption is that data integrity standards have already been adopted here, so we are looking at the residual risk mitigation following that implementation.

![Figure 1: Dynamic modeling of cyber risk](image)

- Green = 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
- Yellow = the move to riskier areas
- Red = the long-tail or black-swan event that could make the entity insolvent

Source: Ultimate Risk Solutions and Risk Explorer

---

2 KSI by Guardtime (www.guardtime.com) is based on mathematical proofs and keyless cryptographic functions approved by the EU and the US National Institute of Standards and Technology (NIST). These proofs and functions withstand exploitation even with advances in quantum computing, meaning that digital assets signed by KSI will have proof information retained over the lifetime of the asset.
The bottom graph shows the situation prior to reinsurance, where small claims are aggregated and a long tail cuts into the companies’ risk-based capital limits. The top graph shows a leaner risk situation after the application of reinsurance, bringing it back in the comfort zone.

The standard deviation process will depend on how the regulator views cyber risk and solvency. Currently, solvency models are geared on average to a 1-in-200-year event, which may be suitable for earthquake and other peril risks but is likely to be different for cyber risks and to vary by country risk appetite.

Other risk transfer mechanisms. In addition to reinsurance, cyber captives are used to address ongoing risk. A point worth noting is the potential to mathematically create a “cyber index” in the same manner that weather 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.

Special-purpose vehicles (SPVs). This risk transfer approach is used in conjunction with capital market investors and sponsors, and it is similar to the catastrophe bond investments that protect countries from earthquake risk. It creates a bond shared by government and private industry to pay and share claims by loss bands in the event of a large or black-swan event. While these partnerships are very effective, such bonds often have a 10-year span, and a shorter life-span vehicle will be more suitable to cyber.

Sidecars. For natural catastrophes, these two-year vehicles have been referred to as sidecars, an SPV derivative of a
captive where investors invest in a risk via A-rated hedge funds. If the event has not taken place within a given time frame, investors receive their money back with interest. This makes cyber risk part of an uncorrelated portfolio investment for 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, 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. Data integrity standards would increase investor confidence in such SPVs.
The industry needs to understand cyber risk independently of the insurer to create the right protection mechanisms, cyber models and rating bands.
The reinsurance industry is known as the secondary insurance market as it provides insurance cover and risk transfer to insurers that the public doesn’t see. 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.

Emerging technology threat
Cyber risk is part and parcel of the transformation of how business is conducted globally, where people interact via smartphones to the commercial internet and social media. Technology has redrawn the boundaries of modern society. The industry must metricize and model the cyber risk correlated with other risks, including cyber risk in the solvency, risk-based capital arena with long-tail exposure reduction.

It is easy for organizations to be reactive to cyber events and say “it will never happen to us,” but 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, share price and a potential rating downgrade.

An incentive to invest
It is difficult for governments to determine if a cyber attack is an attack on a company or on a country. They need to know the extent and nature of the data breach, especially when IP theft or loss of private data is involved. The mechanism being introduced is a mandatory data breach law that forces organizations to report data breaches within a specified period.

Heavy fines (up to 10% of gross annual income) may be imposed for failure to comply, in addition to reputational risk from which companies may take years to recover. Ignorance that a data breach occurred is not an acceptable excuse; the penalties are the same. Based on conversations with clients, EY believes that this is an incentive for companies to adopt and invest heavily in risk-mitigating technologies, standards and leading practices closely related to risk assessment and ERM.

To date, the reinsurance industry has followed insurers in looking at what the risk means and how it can be transferred using existing industry mechanisms (i.e., reinsurance, captives, catastrophe bonds, sidecars and other SPVs).

Cyber catastrophe models and databases
Nearly 60 insurers write some form of cyber insurance coverage outside of errors and omissions insurance (E&O). The reinsurance industry needs to look at the effect of large aggregated cyber attacks that can 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 earthquakes and floods, reputational risk in global financial market meltdowns, health care pandemics and digital data damage caused by large cyber events.

Internal resources have to be deployed to handle the cyber peril. Insurers can offer these services as part of cyber liability cover. Large databases are being developed to access the frequency and severity of attacks containing recent global breaches and recording the associated costs of handling the breach. These event or cyber catastrophe models will:

- Help create cyber XL rates (excess of loss) for reinsurance cover and move away from quota share reinsurance that is required only in the early days of reinsuring a new risk
- Cause the cyber reinsurance industry to mature in the same way it did for natural catastrophe lines
- Include legal expenses, as these are particularly perilous to solvency and to the proper reserving of claims (the ability to pay) over a period

Like all the perils before cyberspace, risk will be subject to regulation and rating. This will force entities down the ERM path if they have not already gone there and will be the defining force moving forward.
Technology, in conjunction with cyber attacks and service providers, makes up the majority of all supply chain disruptions.
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.

A severe cyber attack would affect the global supply chain, especially around commercial and industrial internet usage. Loss of and tampering with data affect the ability to conduct business, disrupt other business contingently related, and seriously impact reputation and associated costs of remediation, litigation and notification of compliance, leading to fines and solvency issues.

The insurance industry knows that the outsource service provider is the main cause of supply chain disruption. This often happens simultaneously, when increasing weather disruption brings cyber and climate risks, which are both large and emerging, together in one event. When service providers outsource to each other, it sends a red alert to the industry.

EY believes that data integrity needs to be embedded in the enterprise, as well as with the IT vendors they outsource to and those outsourcers engage in turn. This is the only way to have an effective subrogation process based on non-repudiation to recover and share fairly the claims incurred from a data breach. It is appropriate to look at how companies might seek to risk-transfer their cyber risk today and then later in the future.
More companies are using cyber captives to help address the ongoing risk of cyber attack.
Cyber captives and risk transfer

Captive insurance is a risk-transfer tool of enhanced risk management that reduces the cost of risk and often provides tax benefits. It is particularly well suited to cyber risks. A cyber captive is an insurance company attached to a parent insurer or group specifically designed to handle the cyber risk of the company. It offers some of these advantages:

- Cyber risk may exist alongside other special risks, such as earthquakes.
- The cyber captive is the occurrence-based policy wording that applies to data breaches occurring during the policy period.
- A longer timeline for claim reporting and payment allows for a build-up of essential captive claim reserves.
- Cyber captives can be used to access the larger reinsurance market for capacity.

Many risk buyers and risk managers are discussing with their brokers the option of using captives for cyberspace so that they can tailor this risk for their organizations 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. 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, access to sound historical data is needed.
The speed of regulatory change in data breach reporting will lead to increased cyber liability cover and even mandatory insurance in some cases.
Within this emerging global regulatory framework sits the rating issue, both at the sovereign and corporate level. Rating agencies can have an economic effect on countries and corporations by making rating changes based on an event. The rating of insurers is also at risk if they do not provide mitigation advice to customers. If a rating drops below a certain level, they will be unable to get reinsurance capacity and will become more exposed to risk. Similarly, reinsurance rating downgrades can restrict access to A-rated capital, meaning the likelihood of defaulting on claims. It is in everyone’s interest in the regulatory and rating space to understand the standards and value that regulators and rating agencies bring to the table.

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

For natural catastrophes, rating agencies look at the use of catastrophe event models that are created by third-party vendors and rely on vendor research and data accuracy. Sometimes these models are blended to get an average view. However, in the case of cyber risk, the catastrophe is the data itself. That requires a broader rating approach (i.e., that of data quality and the IT companies and outsourcers that handle that data).

A data-scoring rating mechanism should be added to the risk assessments for global rating agencies when they measure the ERM effectiveness of the entity they are rating. This means that corporations can take the output of these newly emerging data-rating agencies to compare the internal risk models of the various third parties being used. While they make better risk-mitigating decisions, insurers can make better technical underwriting decisions. The companies using data integrity standards will receive a higher rating, as they have mitigation in place in line with international standards and leading practices.
Leading practices and the Center of Excellence

Insurance companies need to strive for a Center of Excellence across customer, risk-centric and financial activities, as illustrated in Figure 2.

Figure 2: Center of Excellence as an example of big data and insurance

The industry already applies many of these strategies in property/casualty and life insurance, but these can be time-consuming tasks conducted in silos. A shift to data analytics will greatly speed up and correlate these tasks holistically across the enterprise. There is a need to prove trust at the customer level, leverage the knowledge of stakeholders and show transparency in a financial area now heavily regulated and rated. Actuaries are still relied on in this process from top to bottom and are joined by data scientists who add data security and integrity skills.

Data is arguably the most important asset in the insurance industry. Models are only as good as the weakest point in the data. The more analytics and big data become mainstream strategies, the more attention needs to be paid to data quality. This world of security analytics has dovetailed with the fraud, detection and special investigation units, where data analytics has been used for years in the insurance industry. Big data will not solve insurance fraud, but it will enable better questions. It is important that data integrity security innovations be intertwined with these fraud investigations and applied to the next topic of privacy concerns and wrongful collection of data, which are global regulatory fears. This is all part of the trend to move toward intelligence-driven security plans in order to protect digital information assets.

<table>
<thead>
<tr>
<th>Customer Need: trust</th>
<th>Risk-Centric Need: knowledge</th>
<th>Financial Need: transparency</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Distribution channel cross sell/up sell</td>
<td>• Underwriting</td>
<td>• Rating and regulation</td>
</tr>
<tr>
<td>• Customer lead identification</td>
<td>• Product design and innovation</td>
<td>• Asset/liability matching</td>
</tr>
<tr>
<td>• Marketing campaign analysis</td>
<td>• Pricing and deductibles</td>
<td>• Reinsurance optimization</td>
</tr>
<tr>
<td>• Segmentation</td>
<td>• Reinsurance strategy</td>
<td>• Portfolio and asset optimization</td>
</tr>
<tr>
<td>• Know your customer KYC</td>
<td>• Telematics M2M</td>
<td>• Risk-based capital pricing</td>
</tr>
<tr>
<td>• Lifetime value</td>
<td>• Catastrophe models</td>
<td>• Financial modeling</td>
</tr>
<tr>
<td>• Retention and lapse</td>
<td>• Reserving and claims</td>
<td>• Macroeconomics</td>
</tr>
<tr>
<td></td>
<td>• Fraud, SIU and forensics</td>
<td>• Embedded value</td>
</tr>
<tr>
<td></td>
<td>• Subrogation/recovery</td>
<td></td>
</tr>
</tbody>
</table>
No one escapes cyber risk. New, fresh cyber events causing disruption can accelerate laws in countries that haven’t developed their data regulation. EY is seeing that trend in rapidly emerging markets, where consumer adoption of digital technologies is fostering new insurance needs and tighter regulatory oversight. This presents an opportunity for us to help companies better understand privacy, communications and data security regulation and take the necessary steps to protect their business assets.

In the vibrant global cyber insurance market of the future, risk management of a data breach must be built into company policy at the board level and not rely on IT departments. This will give the reinsurance industry the confidence to provide reinsurance capacity to insurers. It will also give capital markets the confidence to draw down capacity to reinsurers to cover cyber risks and provide confidence to investors to place part of their portfolio in the cyber SPV and catastrophe bond space. Moreover, regulators and rating agencies will know that ERM has been included in cyber liability cover.

Cyber liability coverage will likely never cover a global outage of the internet, like a meteorite strike, but the industry will provide risk mitigation and opportunity for businesses to continue their practices protected in the wired and connected world the same way as they were in the past.

EY’s information security services help our clients to assess their security strategies, processes and infrastructure to manage risk and enable compliance with applicable laws and regulations. This includes testing for security exposures and business risks created by vulnerabilities or inadequate systems, applications and network devices.

Protection from cyber risk will require transforming and improving existing security programs and investing in solutions that are yet unknown.

Leading practices should include:

- A pragmatic, risk-based information security strategy that integrates solutions to address business needs, compliance requirements and ERM objectives
- Listening to what is going on in the market, understanding security information trends and threats, and adjusting the risk assessment accordingly
- Continually reassessing new technologies and the threat landscape to confirm that focus is on the right priorities
- Executive and board support that leverages the expertise of partners and vendors and defines which security functions sit in-house instead of being outsourced and in the cloud
- Assurance that information security is an integral part of the risk management function, not a stand-alone unit that fails to involve the business in the process
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2014 EYGM Limited.
All Rights Reserved.

EYG no: EG0201
1407-1283151
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

Our two-part series addresses some important cyber security issues for insurers to consider. Both papers highlight the need for companies to reach beyond what they have done in the past and to develop effective data and risk programs that will protect their businesses from cyber threats in the future. Cyber insurance, security and data integrity and Mitigating cyber risk for insurers are available at www.ey.com/insurance.