How to Use Cyber Risk Quantification to Buy the Right Cyber Insurance

A Buyer's Guide for Executives

AS SEEN IN

Forbes yahoo!finance CYBER DEFENSE MAGAZINE Cybersecurity INSIDERS

Executive Summary

Risk transfer is one of the four main pillars of risk management, next to Mitigation, Avoidance, and Acceptance. These pillars aren't isolated silos, rather they form a cohesive decision-making framework for allocating risk intelligently.

When done right, each approach supports the others:

- **Avoidance** means eliminating risk entirely by not engaging in certain activities. This is useful when potential losses outweigh business value.
- **Mitigation** reduces the likelihood or impact of risks that can't be avoided. This is the main playing field of a CISO.
- **Acceptance** is a conscious decision to retain a risk after mitigation because it's either too small to act on or too costly to mitigate. But this only works if the potential financial impact is known and tolerated by the Board of management.
- **Transfer** (mostly through cyber insurance) shifts specific financial consequences to a third party, but only after understanding what remains after mitigation and acceptance.

Together, these pillars enable a **balanced, financially sound risk management**: avoid when needed, mitigate where practical, accept with full awareness, and transfer (by insurance) what's left.

a. **But what are the main decision criteria for buying cyber insurance which fits with your company's risk management strategy?**
b. **And how can Cyber Risk Quantification (CRQ) help you optimize cost/benefit?**

This whitepaper focuses on the two main decision criteria for cyber insurance, 1) Scope of coverage and 2) Limits of insurance. Both criteria are interlinked, which will be explained in chapter 3.

Definitions

These short definitions will help you understand the insurance terms mentioned in this whitepaper.

- **Consequence scenario:**

  A grouping of cyber threat scenarios characterized by different outcomes of financial losses. Every consequence scenario consists of multiple cyber threat scenarios that cover most discrete cyber incidents. Consequence scenarios modeled by Squalify are Business Interruption, Data Privacy Breach, and Financial Theft & Fraud.

- **Scope of cover:**

  The scope of insurance cover defines the specific financial risks and business impacts an insurance policy will respond to. Such scope is reducing the covered losses in relation to the original risk. It outlines which types of cyber incidents are covered, which costs will be reimbursed, or clarifies any exclusions.

- **Limit of insurance:**

  The limit of insurance is the maximum amount an insurance will pay for covered losses. There are two key types:
  a. Per-event limit: The cap for a single incident
  b. Annual aggregate limit: The total payout cap across all incidents in a year

  Often, the amount for the annual aggregated limit is once or twice the amount of the per-event-limit.

- **Aggregated limit:**

  The aggregated insurance limit is the total maximum payout an insurer will cover across all claims within a single policy period, usually one year. It doesn't matter if one large claim is filed or multiple smaller ones. Once the aggregate limit is reached, no further claims will be paid.

- **Sublimit:**

  An insurance sublimit is a smaller cap within an overall policy limit, applied to specific, often non-standard types of losses or coverages.

- **Deductible:**

  A deductible is the amount an insured must pay before the insurer contributes to a covered loss. The most common type is a per-claim deductible, it applies to each incident separately.

- **Self-insured retention:**

  A self-insured retention (SIR) is similar to a deductible but there's a key difference: With an SIR, an insured company handles the claim directly up to the retention amount. The company manages the investigation, legal response, vendor payments, etc., before the insurer gets involved. With a deductible, the insurer manages the full claim from the beginning, and the insured reimburse the insurer with its portion.

- **Insurance layer program:**

  An insurance layer program is a structured way to stack multiple insurance policies to reach higher coverage limits than a single insurer is willing to provide. It's commonly used for large, complex companies. Such an insurance program always starts with a primary policy with a defined limit (e.g., € 10m). Above such basic cover additional excess layer policies from other insurers extend the total coverage up to the desired total annual aggregate insurance limit. Each layer only pays if the layer below it is exhausted.

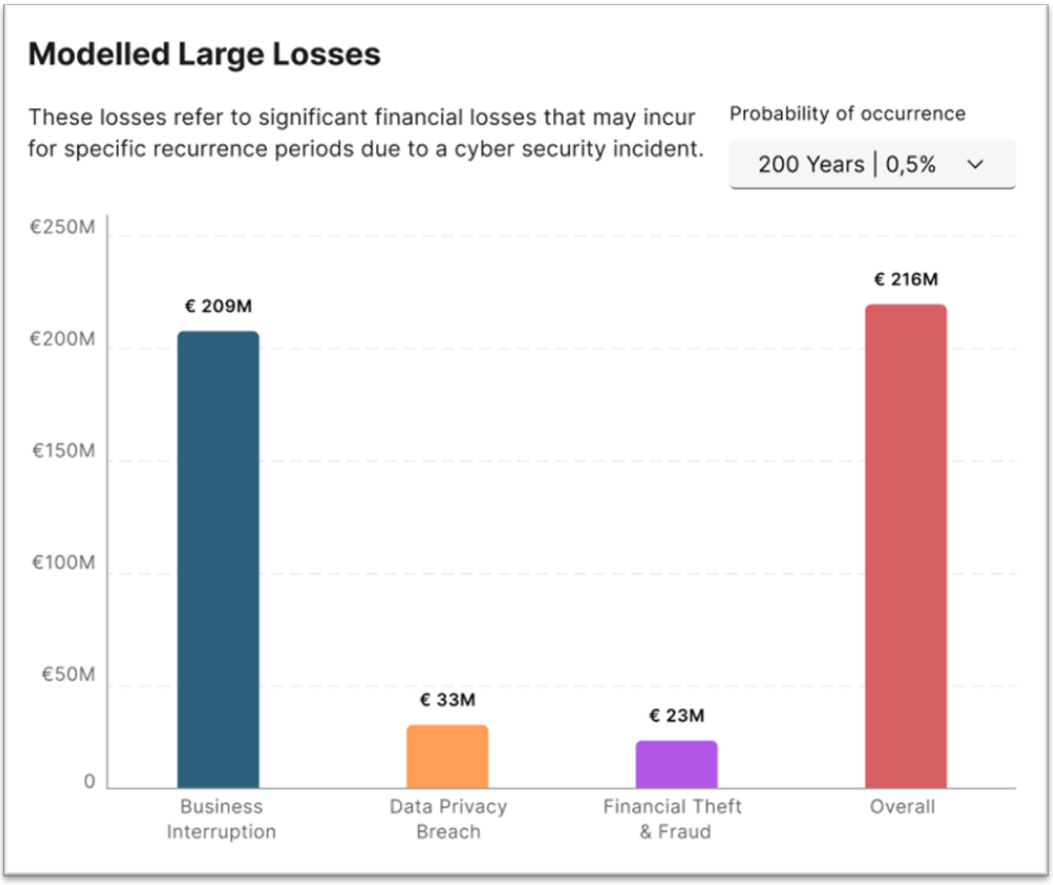
1. Scope of Coverage

Classic cyber insurance covers both first- and third-party risks. The corresponding consequence scenarios are Business Interruption (BI) and Data Privacy Breach (DPB). Sometimes, insurance policies can also include additional financial consequences of cyber incidents, like Financial Theft and Fraud (FTF) by a non-standard coverage endorsement.

Depending on the specific risk profile of a company, often all those three consequences are not equally exposed by cyber risks. Therefore, the first decision is to decide the scope of the insurance coverage within these three options. In most cases BI and DPB are covered together with the same annual insurance limit, and FTF (if it is included at all) is included in such an aggregated annual insurance limit, usually with a much smaller sublimit.

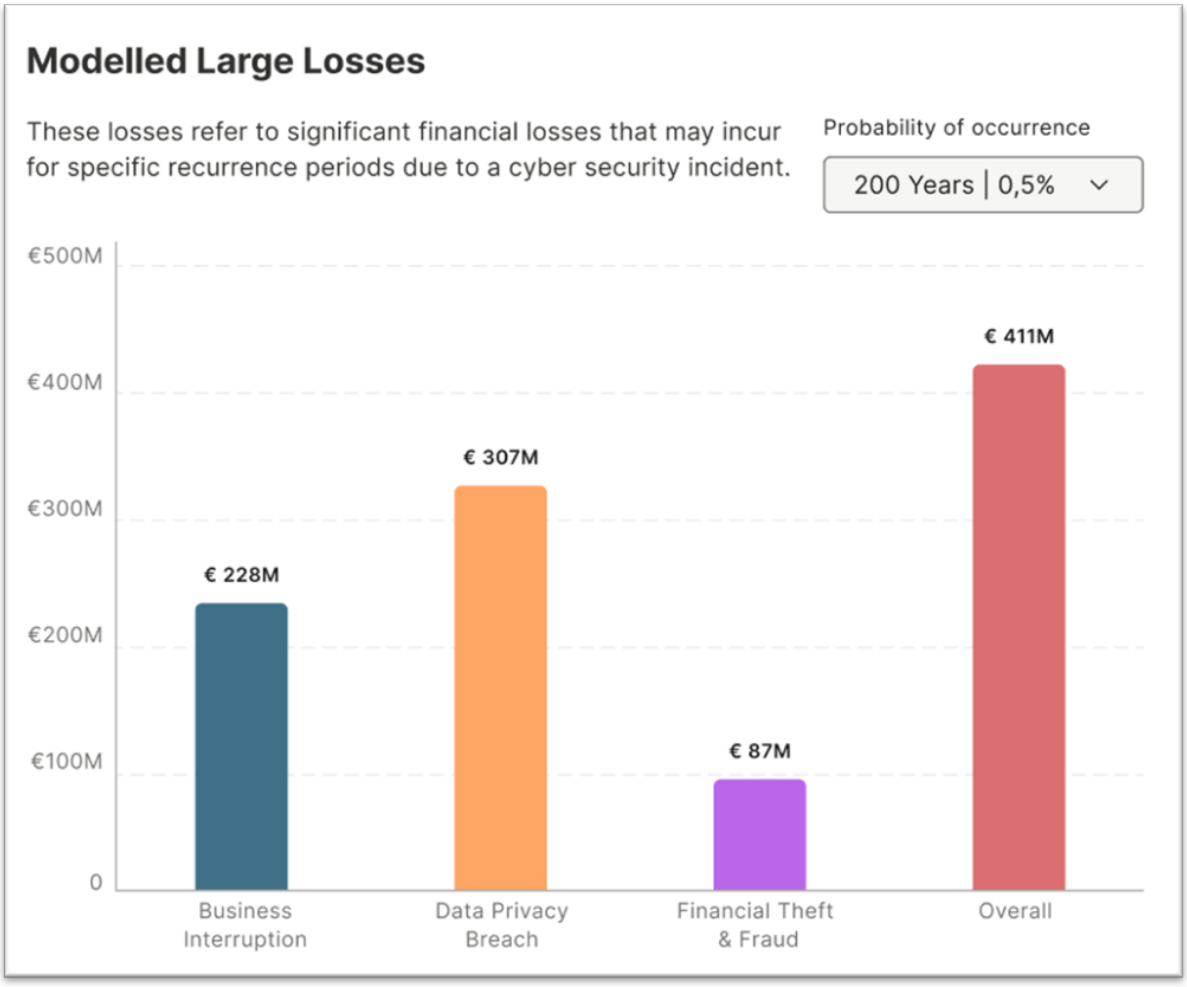
Cyber Risk Quantification (CRQ) can help a company decide which risk scenarios to transfer to an insurer.

For example, if one of these consequences is by far the dominant one, you may decide to buy insurance only for this scope of coverage. In the following example of a medium-sized manufacturer the cyber risk is clearly dominated by the BI exposure:



Based on such a risk profile the company may decide just to buy insurance for BI only.

But in most industries and individual companies the risk profile is characterized in a way that BI and DPB risk metrics are not that different, and FTF significantly lower than BI or DPB, as shown in the following graph for an international Banking Group:



This corresponds with the most common scope of insurance covers of a annual aggregated limit for BI and DPB. Whether to include in such an aggregated limit a special cover for FTF with a lower sublimit depends on the quantified FTF exposure and the risk appetite of the company.

Squalify is ideally placed to support here, because all of our main output metrices are differentiated by BI, DPB, FTF, and Overall.

2. Limit of Insurance

If the scope of coverage is decided the next most significant decision is the extent to which this scope of coverage should be insured. This decision on the annual and aggregated limit of insurance is the most difficult one.

Often **insurance brokers provide benchmark** values about the limits similar companies in a peer group have bought. While this may be helpful, relying on the buying behaviors of the insurance market, this has significant downsides:

- The insurance market is cyclic in relation to the market prices: in “soft market” phases the premiums levels are lower, and companies can buy more insurance limit for a given budget, while in “hard market” phases the premiums levels are higher, and companies will need to settle for buying less limit for a fixed insurance budget. Thus, benchmark limits reflect rather market condition than coverage based on risk.
- In addition, benchmarking recommendations can be inaccurate if the company has a different risk profile in view of scope of coverage and financial exposures compared with its peer group.

Thus, peer benchmarking provides a picture of the insurance market rather than your company-specific risk exposures and risk appetite. Cyber Risk Quantification (CRQ) is the better solution for the decision on insurance limits because it is based on company-specific risk exposures.

With Squalify’s Top-down CRQ methodology there are in principle four different risk metrics available to support insurance buying decisions: a. Worst Case Loss, b. Modelled Large Loss, c. Modelled Average Loss, and d. Annual Loss Expectancy:

a. Worst Case Loss (WCL)

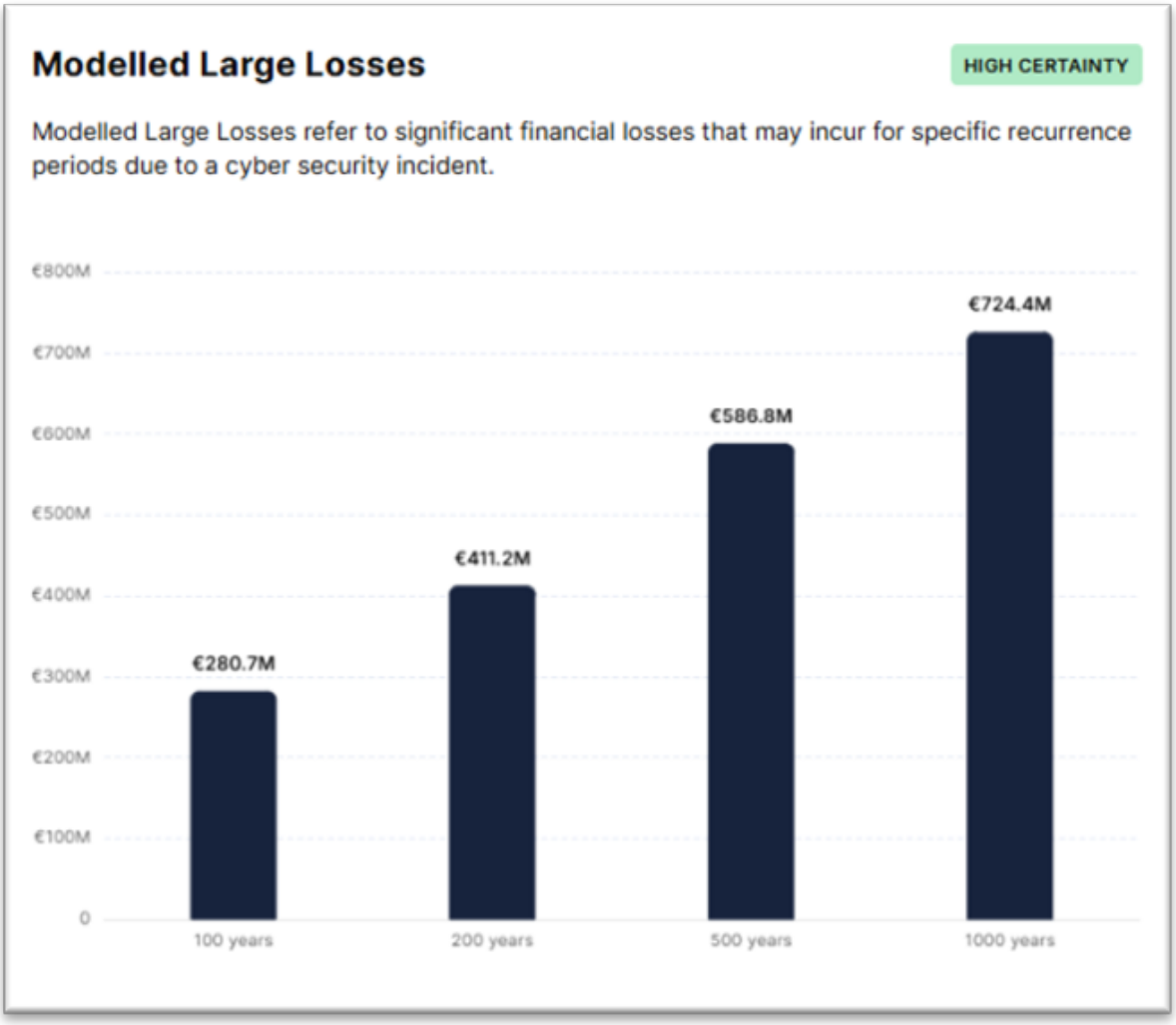
The WCL is calculated under the assumption that almost all controls fail. In insurance language this is similar to the “Probable Maximum Loss” (PML). In first-party (Property) insurance the PML often determines the insurance limit. In cyber insurance a company (with a low risk tolerance) may choose the WCL to decide the insurance limit for BI.

b. Modelled Large Loss (MLL)

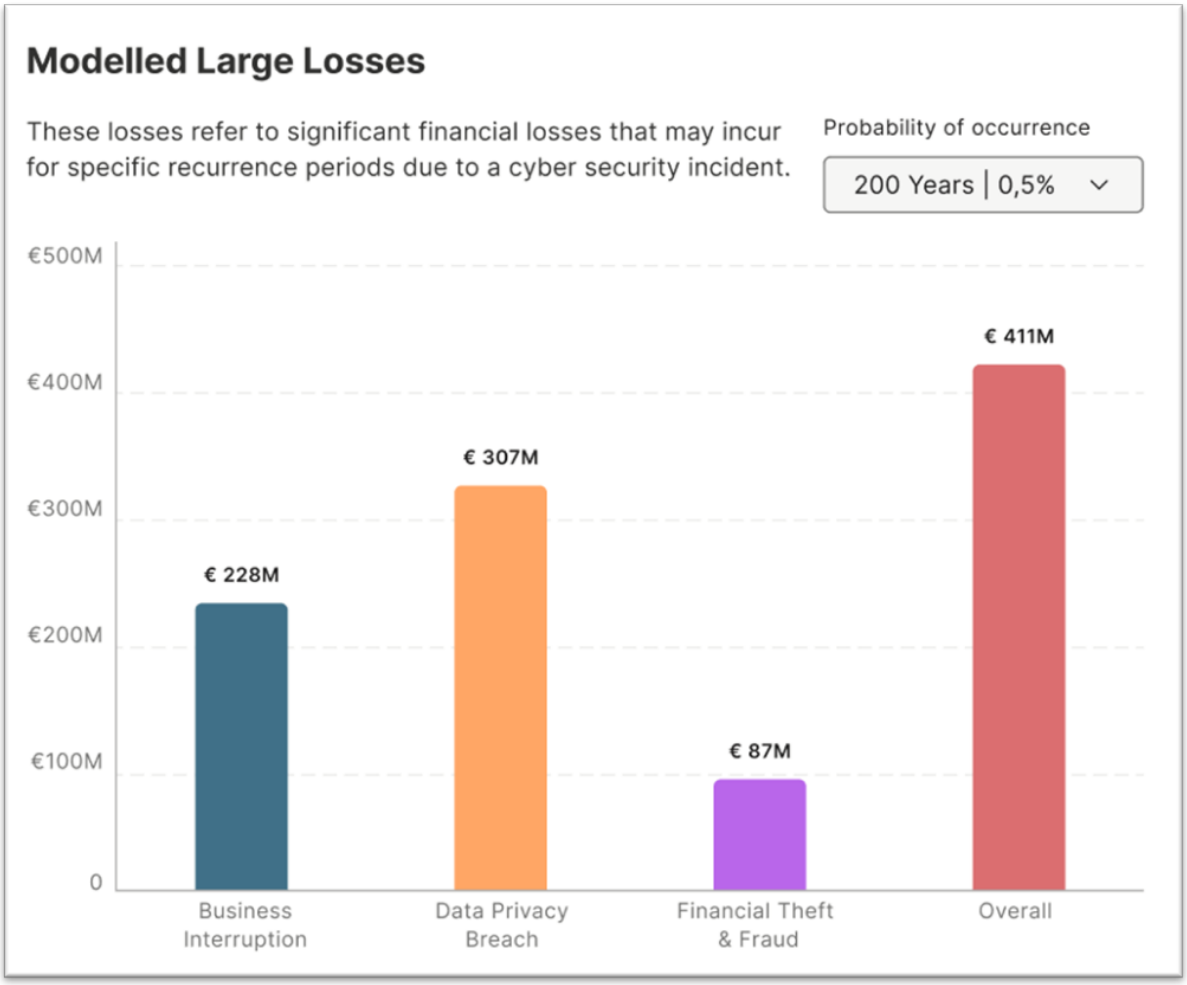
The Modelled Large Loss is calculated in the Squalify platform by incorporating the information security maturity of a company into the quantification model. Thus, how well a company is protected against cyber incidents reduces both the loss potential compared to the Worst Case Loss significantly, and the probability of occurrence. The statistical term for the MLL is Value-at-Risk (VaR).

The Value-at-Risk that must be modelled by a company may be defined by regulation in some industries. But in general, for the rare but most severe loss scenarios, companies chose a specific probability in line with their risk tolerance. Typical probabilities for the risk tolerance of large companies are 2%, 1%, or 0,5%, or when expressed as a recurrence period, are 1 in 50, 1 in 100, or 1 in 200 years.

In our example of the Banking Group the MLL values are displayed as follows in the Squalify platform:



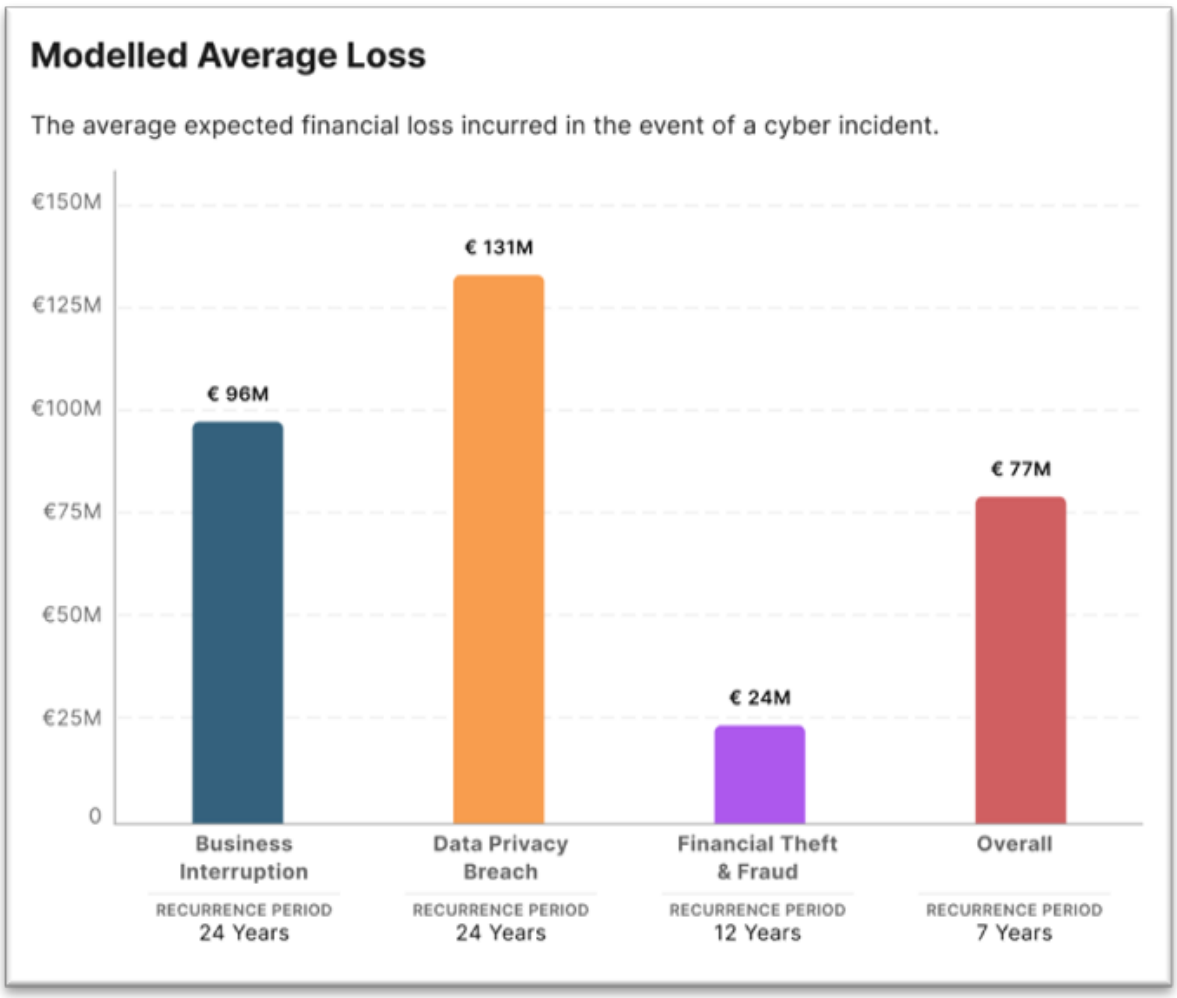
If, for example, a company manages risks with a VaR recurrence period of 1 in 200 years (which equals a probability of 0,5%) then a cyber risk profile – differentiating the consequence scenarios BI, DPB, and FTF – could look like this:



In such circumstances, an annual, aggregated insurance limit for all three consequence scenarios BI, DPB, and FTF should not significantly go beyond € 400m. This would mostly cover the overall 0,5% VaR of € 411m. This would include severe scenarios like a double-hit ransomware attack resulting in a BI and DPB loss. Assuming, for example, that for FTF an insurance sublimit of € 50m is bought, such a limit would cover the expected overall loss amount almost completely.

c. Modelled Average Loss (MAL)

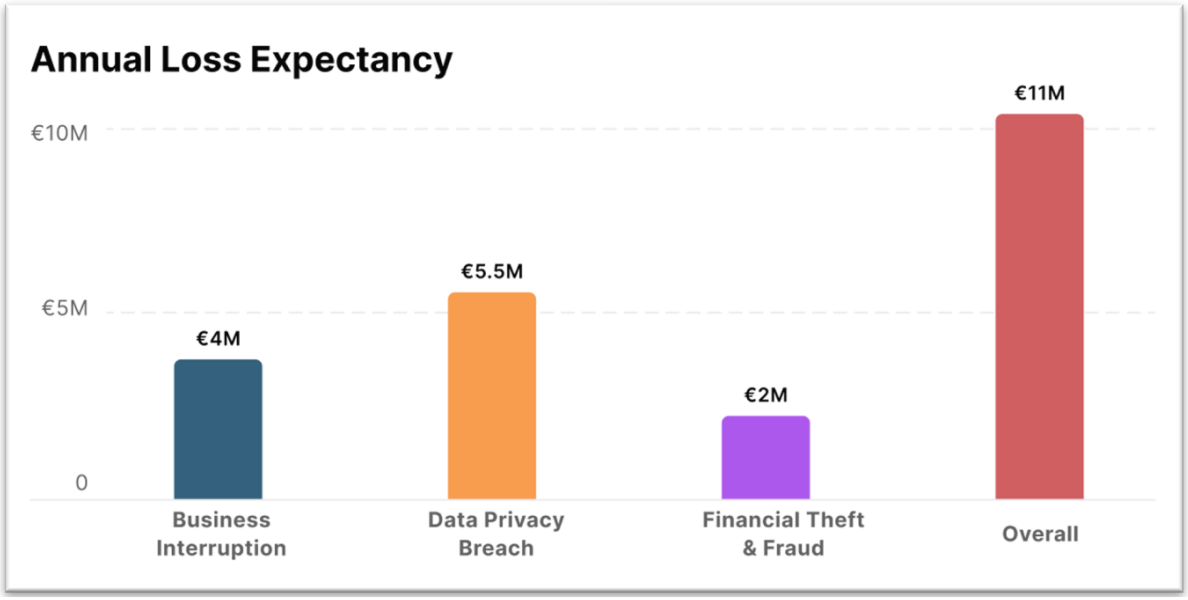
The Modelled Average Loss describes how often on average a cyber incident may occur, and if it occurs the expected financial loss on average. This metric supports the management of financial buffers for cyber incidents in the medium term. In our example the Overall MAL is € 77m every 7 years:



Typically, CFOs would establish a kind of financial buffer of € 77m for cyber incidents (e.g. on balance sheet or planning level) as an alternative to a cyber insurance cover.

d. Annual Loss Expectancy (ALE)

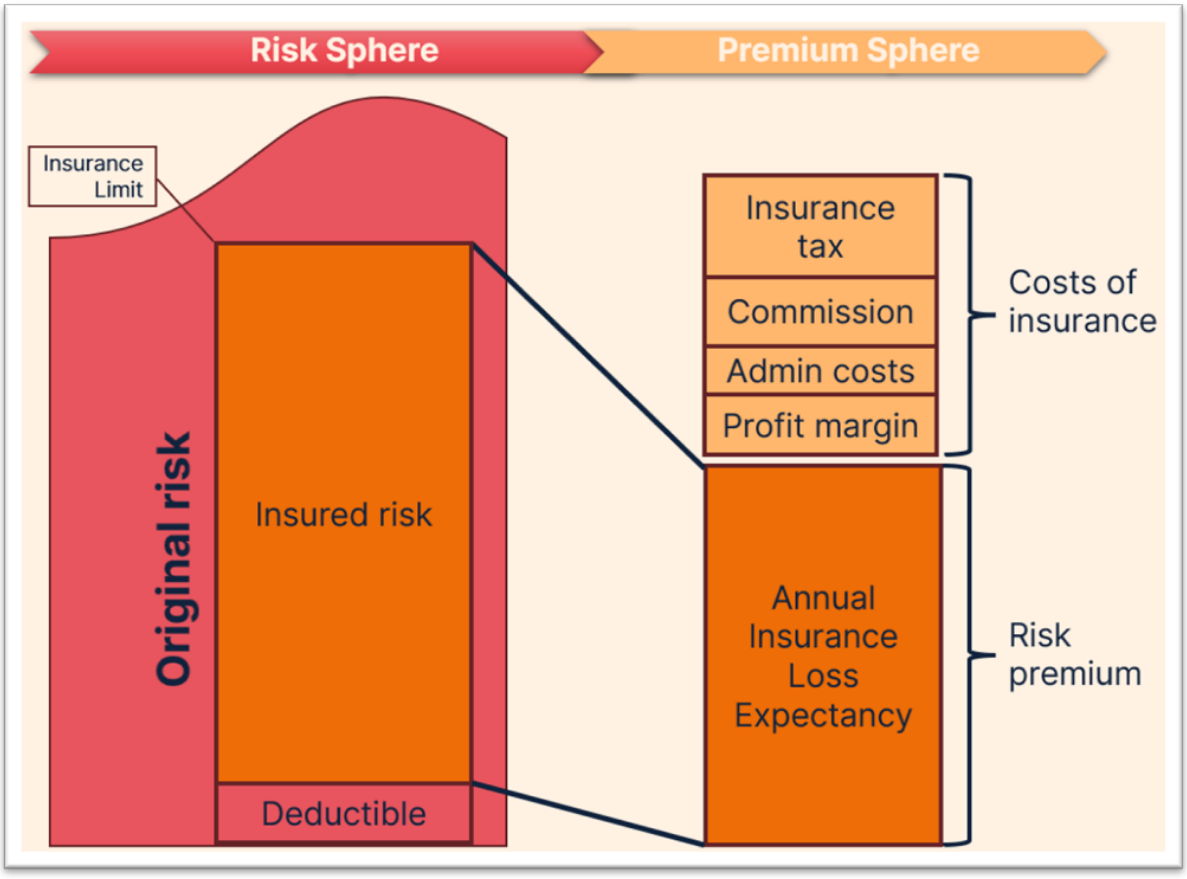
This metric can be calculated by dividing the Modelled Average Loss by the Average Recurrence Period. The Annual Loss Expectancy is the average financial loss burden a company faces per year. In our example the Overall ALE is € 11m (€ 77m / 7 years):



From a CFO point a view, the ALE is the annual amount to set aside to fill the overall average financial buffer for Cyber incidents as calculated with the Modelled Average Loss (i.e. € 11m over 7 years to accumulate to the MAL of € 77m, see above).

Insurance policies typically run for one year and as such it is sometimes assumed that insurers use the ALE to set the premium of cyber insurance. However this is not the complete picture. It is important to understand that insurers and companies planning to buy cyber insurance use risk quantification in different ways.

Both wish to understand the potential costs of incidents, but insurers can exclude certain aspects of this “orginal risk”, mainly by insurance limits, deductibles and the scope of insurance (e.g. trigger definitions, obligations, exclusions). In addition, the risk alone does not dictate the policy price as insurers need to accommodate further costs in the final price, e.g. for costs of administration, sales, and profit margin:



Therefore, the ALE calculated with Squalify can be seen as a rough indication for any insurance premium only.

3. Combined View on Scope of Coverage and Insurance Limit

For the final decisions on buying cyber insurance both the scope of coverage and the limits of insurance need to be considered together.

The first decision is on how to cover the classic scope of a cyber insurance, i.e. business interruption (BI) and/or data privacy breach (DPB).

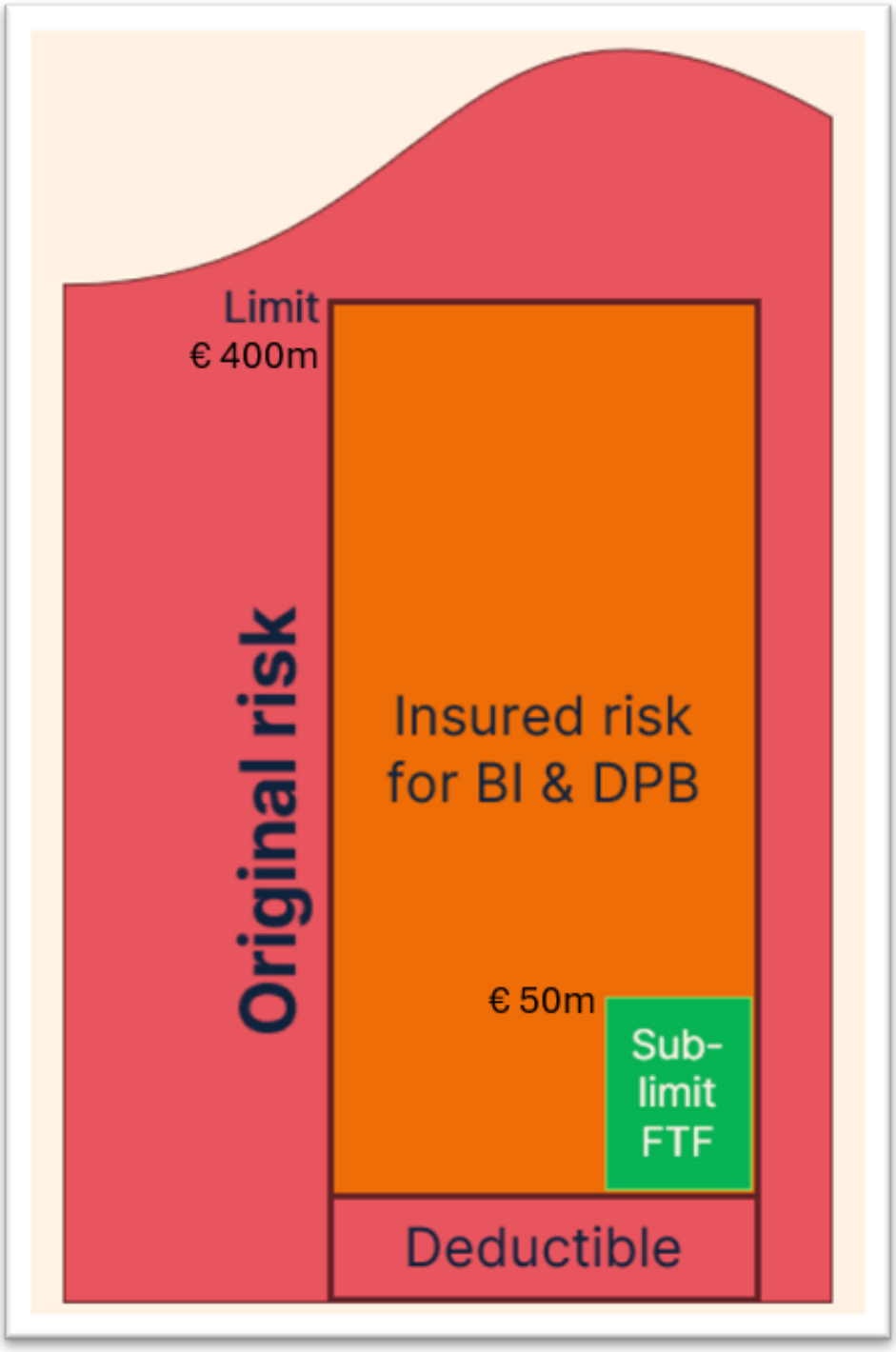
a. In case there is **one of these consequence scenarios dominating** you may decide to buy insurance only for that scope. In the following example the company may buy a cyber insurance for BI only with an annual insurance limit of € 200 m:

b. If **BI and DPB are not that differently exposed** the company may buy an annual aggregated insurance limit for both consequence scenarios considering the Overall Modelled Large Loss metric as in this example of an international banking group:

Because the Overall MLL of € 411m includes some risk potential for FTF a limit of € 400m is sufficient to cover the aggregated exposures from BI and DPB (ex FTF) completely.

c. **Financial Theft and Fraud is a special insurance** cover which can be included with a smaller limit (also called sublimit) within the overall annual and aggregated limit of insurance for BI and DPB.

For some industries there are also separate covers available, e.g. Crime insurance or Bankers Blanked Bond policies (BBB) for financial institutions. Those covers usually have a different scope and are handled in other insurance markets which may have advantages for the insured. While all these covers have a different scope of coverage you may use the MLL for FTF as a criterion for selecting whether purchase such coverage at all and if yes, to what extent in view of the Cyber part.



In this example of the international Banking Group the company may decide to buy a sublimit of € 50m for an FTF endorsement to the classic cyber policy. Typically, such sublimit is part of the overall annual aggregated limit. That means that any losses paid out for FTF will reduce the remaining limit for all other loss types within that policy year.

4. Additional Considerations

4.1 Deductible

A deductible is the amount an insured company must pay before the insurer contributes to a covered loss.

A risk transfer for frequent and smaller cyber losses makes in most circumstances no sense from an economic point of view. Insurers' premium loadings make coverage of such a highly predictable loss burden not worth insuring. Therefore, deductibles or self-insured retentions (SIR) are effective coverage elements to eliminate smaller losses from insurance and focus more on risk transfer of the potential losses from large and extreme cyber incidents.

Large companies often decide for deductibles between € 0,5m and € 10m, sometimes even up to € 20m.

It is recommended to ask the broker and insurers for premium quotes for different deductible options to find your sweet spot. As a principle: for a given limit, increasing the deductible will reduce the premium, however there are some nuances to consider.

4.2 Premium vs. Insurance Limit vs. Deductible Relation

The main driver of selecting the insurance limit is the premium the insured company is willing to pay. Here, there are different approaches available:

- **Insurance budget:** In case the insurance buying department works with a fixed budget they can spend for cyber insurance per year, they would optimize the relation between limit and deductible. In this case they often have defined a minimum limit they want to buy strategically, and have more flexibility on the deductible which is anyhow by far the most sensitive driver for the premium. The premium per each million of limit is very high for smaller losses (with high frequency) compared to limits at the top of an insurance layer program.

  With a fixed premium budget the insured will typically buy less limit and/or higher deductibles in a "hard market" (i.e. when the market prices are high) and more limit with lower deductibles in a "soft market".

  If the market pricing does not allow to buy the minimum limit the company may decide not to buy insurance for that year.

- **Fixed insurance limit:** Such a minimum limit is mostly defined by the strategic risk appetite of the company. Buying this limit to the different premium levels depends very much on the market cycle. In this situation

the size of the deductible is an important factor to balance out economically feasible premium/limit relationships. In this case the decision of not buying insurance is a valid option, especially in a hard market situation.

4.3 First Buying vs. Renewal Decisions

Strategic and tactical decisions on cyber insurance need to be made both for the first time buying a coverage or before any annual renewal of an existing cyber policy (as most cyber insurance coverages for larger companies are re-negotiated every year).

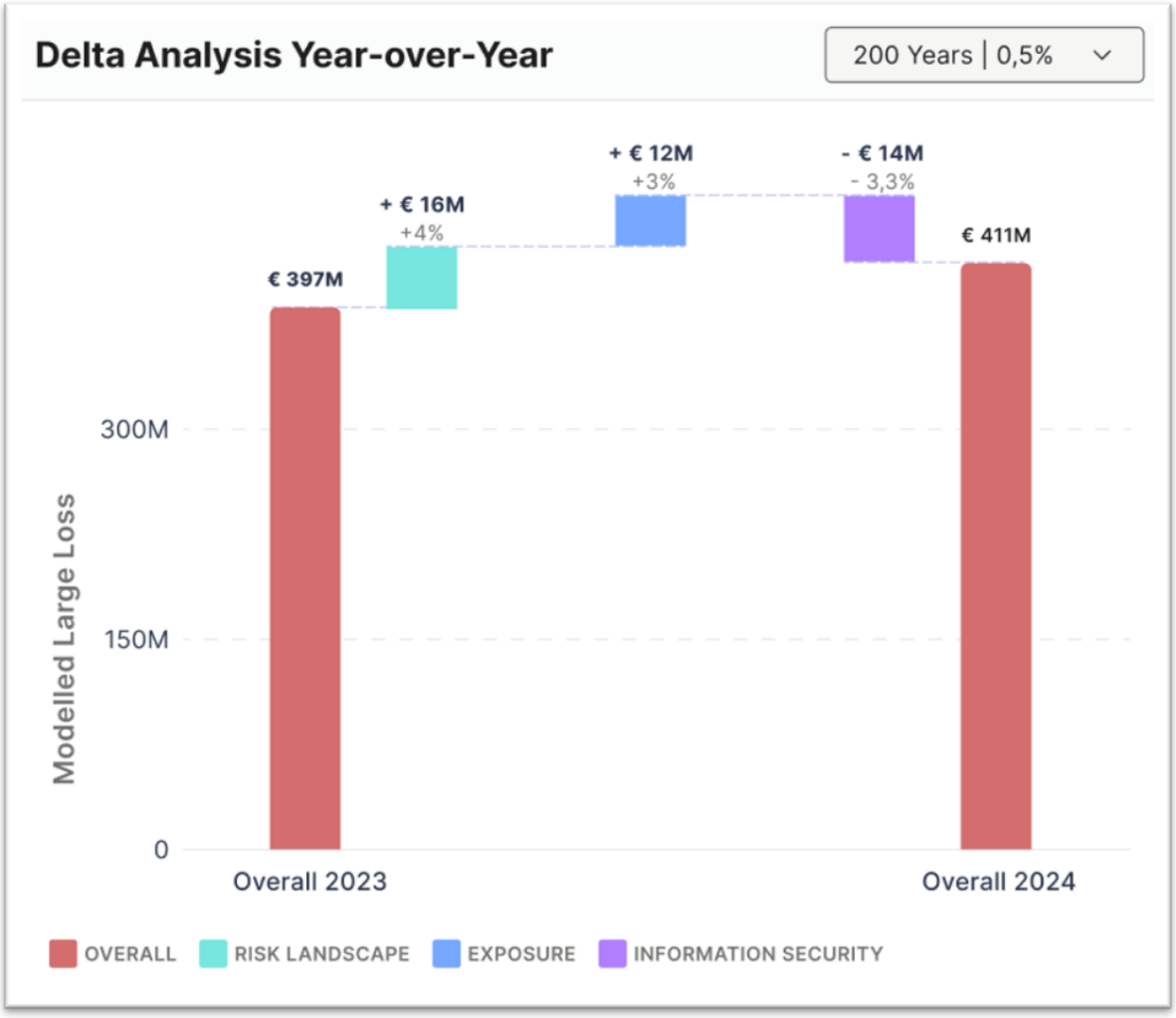
In case of the first purchase of cyber insurance, the discussion earlier in this paper describes how the Squalify approach can help with your decision making.

Additionally, in case of renewals, Squalify can help you to compare the proposed changes in premium and conditions with the changes in the original cyber risks of your company.

Squalify provides a Year-over-year Comparison which explains the three main risk drivers for the changes of risk from one to the next insurance period:

- Changes of the risk-landscape, e.g. new threat vectors, hacking strategies
- Changes in company exposures, e.g. turnover, business model, market shifts
- Changes in the company's InfoSec maturity, e.g. by implementation of control improvements

In our example the analysis shows that the improvements in InfoSec maturity could compensate only partly for the increases in the threat environment and the company growth:



This analysis provides valuable insights for your own internal renewal decisions but may be also used to better negotiate with the insurers. Because cyber insurers typically also analyse the changes to the previous year during the renewal phase, a Squalify Delta Analysis enables the insured to prepare for these conversations, to “talk the same language” and negotiate on eye-level.

5. Final Words

When buying or renewing a cyber insurance policy it is important to understand what scenarios to cover, and how much limit to buy. Top-down CRQ is the best way to support your insurance buying decisions based on your company-specific risk assessment.

Squalify's CRQ platform makes strategic decision making possible on whether and to what extent to use risk transfer, which fits your risk appetite, be it for the first time or at any insurance renewal.

Book a meeting to learn more on how you can use the Squalify platform to inform your insurance purchasing decisions for your company.

About Squalify: Cyber Risk Quantification for the Boardroom

Squalify is a cyber risk quantification platform for the Boardroom. Our risk insights support information security and risk executives to answer the Board's toughest cybersecurity questions and steer group-wide risk reduction effectively from one platform. Fast. Data-backed. Scalable.

We are a corporate venture of **Munich Re**, one of the world's largest cyber reinsurers. Our proven risk model is built on a decade of cyber insurance expertise and powered by exclusive access to Munich Re's industry-leading cyber loss database; covering over 100,000 companies across 130+ industries and 80 countries. More than 4,500 companies have already been assessed using our quantification methodology.

- Book a meeting
- Learn more on www.squalify.io
- Follow us on Linkedin
- See what Forbes is saying about us

AS SEEN IN