Deloitte.

Cyber insurance underwriting

Helping boards create supervisory confidence

CENTRE *for*
REGULATORY STRATEGY
EMEA

Contents

Introduction

Who is this report for and what does it set out to achieve?

This report provides a practical perspective on how general insurers can meet regulators' and supervisors' developing expectations for management of cyber underwriting risk. Cyber underwriting risk is attracting increasing regulatory attention and scrutiny because it can pose material levels of aggregate risk for many general insurers. We hope this report will be useful for non-executive and executive directors seeking to challenge the practical steps their firms are or should be taking to manage these risks in line with regulatory expectations, as well as those with day-to-day management responsibility for cyber underwriting risks, for example Heads of Underwriting or Claims.

As part of our research we conducted interviews with experts from the front line of cyber underwriting at leading insurers and brokers, as well as experts in Deloitte's financial services practice. The EMEA Centre for Regulatory Strategy is most grateful to those who gave their time and expertise to be interviewed for this report.

How to use this report

Each section of this report contains:

- Key risks and potential actions for firms.
- Positive and negative indicators that supervisors may look for in their interactions and assessment of firms' maturity with regards to cyber insurance underwriting.
- Example questions that Board members may ask to challenge their organisation's understanding of, and approach to, managing cyber underwriting risks.
- A check-list of potential next steps to help build supervisory confidence in firms' understanding and management of cyber underwriting risks.

Executive summary

Despite the relatively small size of the stand-alone global cyber insurance market (€295 million GWP in 2018), cyber insurance has come under increasing regulatory scrutiny due to concerns around the rapid growth of the market and the uncertainty of expected losses against which firms have to reserve and hold capital. Whilst the UK's PRA has taken a leading role from the outset, other national supervisory authorities, including the ACPR in France and BaFIN in Germany, have increasingly voiced concerns around cyber insurance. At the EU level, EIOPA is developing its response through a cyber underwriting strategy.

This report has three sections. Each looks at a key area of risk that we expect to be of prima facie regulatory and supervisory concern. The sections we cover in this report are:

1. Identifying and managing silent cyber exposures

Supervisors are concerned that insurers may be unaware of the full extent and nature of their cyber exposures. Insurers need to identify, quantify, and manage their cyber exposures according to regulatory expectations and amid competitive pressures, while maintaining a firm eye throughout on consumer protection. The COVID-19 pandemic is also likely to influence regulatory expectations and drive commercial demand for more transparent cyber coverage, given the debate it has sparked around the scope of business interruption insurance coverage following extreme events. Firms should take into account any lessons learned from previous experiences, and review policy wording accordingly.

2. Managing modelling and data risks

Modelling cyber risk is inherently extremely challenging due to such factors as the lack of available and standardised cyber incident data and the rapidly changing nature of the risks. To address supervisory concerns, insurers will need to demonstrate the robustness of their approach to modelling cyber risks and that strong model risk management disciplines are being applied to meet the specific challenges of cyber models. Chief among these will be robust model validation based on qualitative and judgmental analysis and challenge; controls around the use of expert judgment; using realistic disaster scenarios to understand the impact of extreme events; appropriate management of external models; and improving data collection and use capabilities. Firms should devise a strategy that makes the most efficient use of one of the most scarce resources: expertise.

3. Managing tail risk

The relatively low incidence of cyber events and the changing nature of technology create uncertainty about the nature and scale of 1-in-200 year (or any other calibration) cyber events. Supervisory authorities are concerned that, without a solid handle on the first two issues covered by this report, firms will find it very difficult to manage their exposures to low-probability, high-impact events. Firms will have to demonstrate that they understand and can manage effectively their peak and accumulation cyber risks, and that their reinsurance arrangements will work as intended and reflect the board's risk appetite.

Identifying and managing silent cyber risk

- Silent (non-affirmative) cyber risk refers to cyber risks implicitly covered by “insurance policies that do not explicitly include or exclude coverage of cyber risk”[1].
- Absent exclusions, cyber events could trigger claims on policies that may not have been designed and priced to cover cyber risks.
- As the crystallisation of silent cyber risk could lead to significant losses for the insurance industry, prudential regulators have been increasingly vocal about the need to identify and manage these exposures.
- From a consumer protection perspective, providing transparent coverage is also essential. Firms will have to design carefully their silent cyber strategy to strike the right balance between managing exposures and providing useful cover, amid commercial pressures that may complicate certain mitigation strategies, such as using exclusion language or requesting larger amounts of data from a potential policyholder.

90% of $3 billion

NotPetya cyber attack insurance losses relating to non-affirmative cyber risk.

“Global insurers have slowly started to analyse silent cyber as an issue and formulated a mitigation plan, but the execution has been inconsistent at times.”

Interview with cyber insurance broker, 2020

[1] Cyber insurance underwriting risk Supervisory Statement 4/17. PRA, 2017

Identifying and managing silent cyber risk

Key risks

- Cyber insurance is an aggregating class. For example, a ransomware attack may trigger multiple types of policies. Firms with a limited view of their non-affirmative cyber risks may find that their exposures are beyond their risk appetite.
- The process of addressing silent cyber risks is simpler for certain classes of business than others. For example, using simple wordings exclusions might significantly dilute the usefulness of a D&O policy. Firms nonetheless need strategies to exclude cyber risks or make them explicit, and potentially to mitigate exposures.
- Firms that do not encourage cross-functional and cross-class collaboration, and effective use of often scarce expertise and resources, may have limited views of their aggregate silent cyber exposures. The board's leadership, and the design of the overall strategy to address silent cyber, will be key.
- Reliance on manual processes may create additional complexities in implementing strategies to deal with a peril affecting multiple lines. This may create difficulties in collaboration, which could affect the quality of board MI. Different classes may end up using different definitions of what constitutes a cyber risk. Designing an appropriate overall strategy and overseeing its effective implementation across the different relevant departments will thus be crucial.

Actions for firms

- Supervisors will want insurers to understand their exposures to cyber risk, including silent exposures, and use this as the basis for their overall cyber insurance strategy.
- Policy language around cyber risk should be kept clear and simple in order to avoid ambiguity or misunderstanding amongst policyholders. In the medium-term, convergence in wording across insurers would facilitate the comparison of policies and could contribute to more consistency in the treatment of claims across the industry.
- Increased cross-team collaboration should contribute to creating effective feedback loops. The claims function in particular needs to be able to identify claims linked to cyber events, and feed this back to the underwriting function.
- Regulators consider the insurance market to have been insufficiently proactive about silent cyber. For example, an EIOPA survey found 41% of insurance groups do not have an action plan in place to review their portfolio in the context of cyber exposures and, if necessary, reword the contracts.
- The PRA found firms appear to have very different perceptions of where non-affirmative cyber risk losses might occur. 25% of firms attributed the majority of losses of the PRA's most recent stress test to property covers, while 45% deemed the cost would mainly come from D&O and E&O policies. Though some of this may be attributed to differences in firms' portfolios, firms still need to be able to provide a rigorous analysis and quantification of their unique silent cyber exposures.

Identifying and managing silent cyber risk

Positive supervisory indicators

- Responsibility for embedding the silent cyber mitigation strategy across the business is clearly allocated, backed by demonstrably strong senior buy-in.
- Silent cyber risk exposures have been discussed and taken into account in the board's risk appetite. The board has developed and implemented explicit strategies to manage silent cyber exposures.
- The board has done a deep dive into silent cyber exposures, to validate the strategies it has developed.
- Cyber premiums and losses are tracked across the business, for example through specific codes used by underwriters to tag policies across business lines.
- There is evidence of cross-team collaboration and training, e.g. ensuring claims functions have the right skills to distinguish and escalate non-affirmative cyber claims.

Negative supervisory indicators

- The insurer has not set aside reserves for cyber risk for a given line of business, and is unable to demonstrate that it has taken sufficient steps to justify any assertion that it is not exposed to cyber risk.
- The firm is unable to specify or explain the portion of the premium that relates to the cyber risk in a policy.
- Information and analysis on silent cyber exposures is not captured in board management information and therefore does not inform risk appetites.
- Policy coverage is unclear or ambiguous and so is open to challenge/ interpretation. Policy coverage is inconsistently applied for given contractual terms.
- Managing silent cyber risk is a 'side of desk' project led by individual business lines.

Identifying and managing silent cyber risk

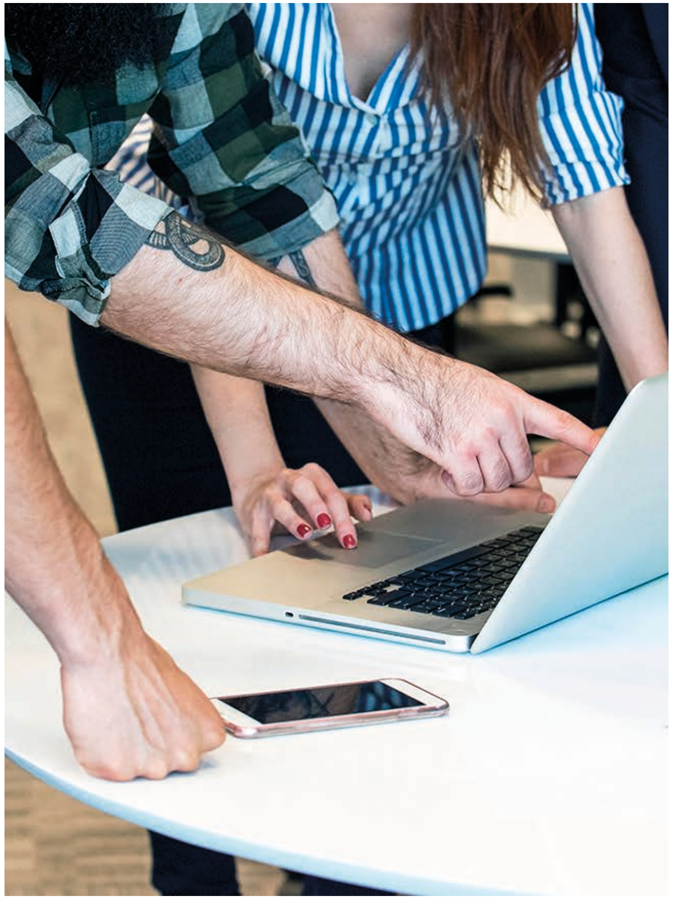
"[...] more ground needs to be covered by firms especially in relation to non-affirmative cyber risk management, risk appetite and strategy."

PRA Dear CEO letter, 2019

Each insurer's strategy will need to fit its unique business model and exposures. However, in our experience, strategies that can be applied effectively to address silent cyber exposures commonly include the following. Many of these approaches featured prominently in our conversations with cyber underwriters at leading insurers during our research for this report.

- Excluding and then reintroducing cyber risk into add-on policies with appropriate limits.
- Removing cyber risk completely and redirecting policyholders towards standalone cyber policies, underlining potential ancillary benefits.
- Splitting up cyber risks that can remain within the policy (e.g. physical damage in a property policy), and the parts of the policy that should be dealt with separately in a stand-alone policy (e.g. non-physical losses in a property policy).

Identifying and managing silent cyber risk



> *"The lack of quantitative assessment of non-affirmative risks combined with a generalised absence of cyber exclusion practices and action plans suggest insurers are currently not fully aware of the potential exposures to cyber risk."*

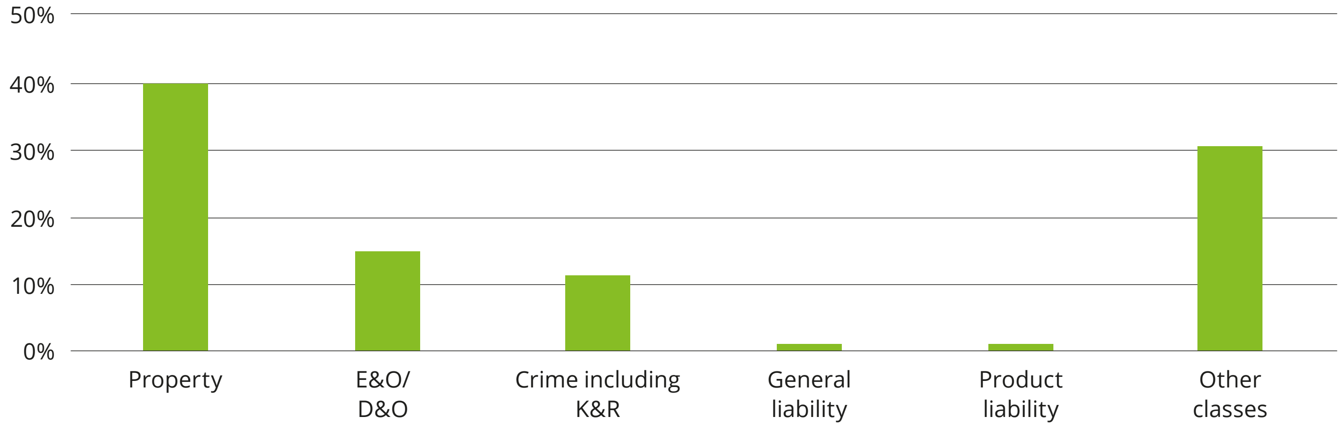
EIOPA. Cyber risks for insurers – challenges and opportunities, 2019

Questions for boards

- How are we making sure that we are identifying and accurately quantifying silent cyber risk exposures in our different lines of business?
- Where we identify no silent cyber exposures, is that conclusion built on rigorous investigation and analysis?
- How are the claims and underwriting functions collaborating to identify where cyber risks are arising in our book? How are we using this information to form a better understanding of our exposures?
- Do we understand where we have and have not excluded cyber risks, and is this clear to our policyholders?
- How do our pricing and capital models take cyber risks into account?
- What is our strategy to address non-affirmative exposures? Have we identified sectors or business lines that are particularly problematic in terms of addressing silent exposures? Why are they problematic and how are we proposing to deal with them?
- How are we balancing customer needs and the need to limit our exposure to cyber risks?

Identifying and managing silent cyber risk

Non-affirmative cyber losses product breakdown



Source: Bank of England IST 2019.

> *"BaFin considers it necessary for insurance undertakings to examine more thoroughly whether cyber incidents were the actual cause of damage [when analysing claims]."*

BaFin Supervisory Programme: Insurance Supervision, 2020

Our conversations with practitioners showed the importance of having a formalised strategy and process in place to address silent cyber, implemented consistently across the organisation. When the process of creating and adjusting policy wordings is informal or poorly controlled, this can lead to 'blind spots' that are not picked up by the firm. Furthermore, if an informal process relies on a few key people, other priorities – or even simple absences – can lead to inadequate policy language being reintroduced into policies without proper escalation or oversight, effectively meaning silent cyber 'creeps back in'.

Identifying and managing silent cyber risk

Checklist for boards

- ✓ Develop a strategy to identify silent cyber risk in policies and quantify the individual and aggregate exposures. The strategy could involve creating a central team composed of members of the underwriting, claims, and legal functions. These could be tasked with creating the processes, systems, and controls to embed the strategy across underwriting classes and business functions.
- ✓ Improve feedback loops between claims and reserving by escalating cyber event claims to better understand where there are potential exposures.
- ✓ Risk appetite: identify silent cyber exposures, incorporate into risk appetites and feed these through to the underwriting function.
- ✓ Re-visit risk mitigation programs in light of silent cyber risk exposures to ensure appropriate coverage is in place.
- ✓ Clarify policy language to make clear what is included and what is not, weighing the need to limit exposures with providing useful cover to the insured.

> *"The most obvious way of dealing with indirect cyber is to simply exclude. The most reasonable way of doing it is to exclude the risk and then build it back in with limits."*

Interview with cyber underwriter, 2020

Managing modelling and data risks

"This underlines the large uncertainty in cyber, the lack of reliable claims data and the immaturity of available models with potential links to capital adequacy."

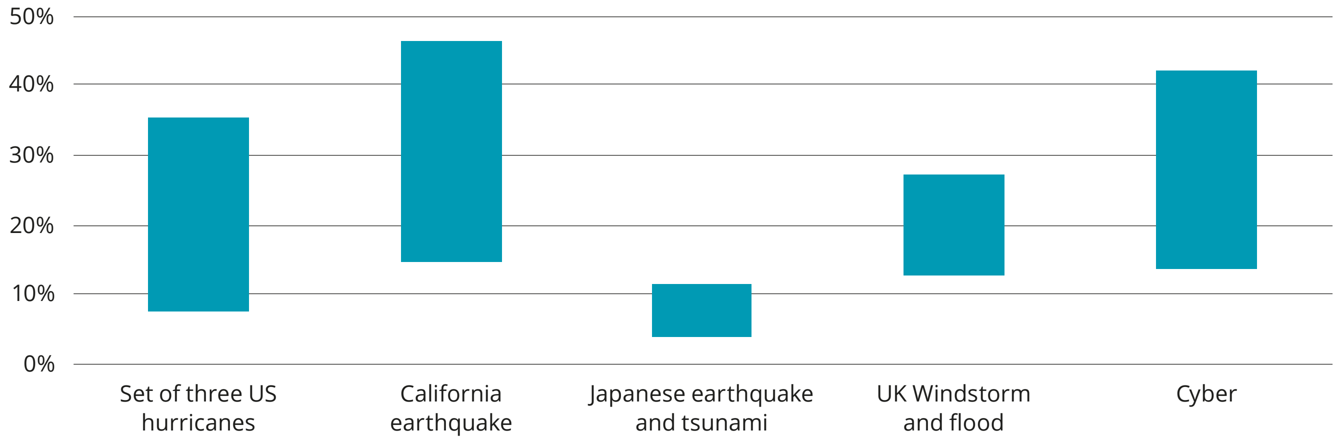
PRA Dear CEO letter, 2019

- The lack of readily available and standardised cyber incident data presents a crucial constraint and hence risk for insurers seeking to create robust models to predict cyber losses.

- While some firms are confident in their market pricing methods for cyber risks, in our view the market overall is still in the process of developing robust technical pricing capabilities, and relies heavily on qualitative expert judgement. Developing the risk profile for cyber insurance is particularly challenging given the evolving nature of cyber risk.

- Managing and overcoming risks posed by data and modelling is crucial for insurers exposed to affirmative or silent cyber risks. Some authorities have suggested industry data-sharing tools as a potential solution, although our research shows firms have mixed views about regulator-led data-sharing solutions.

Midspread impact of PRA stress test scenarios on Ratio of Net losses to Eligible Own Funds



Source: Bank of England IST 2019.

"We believe that we need to develop at European level a standardised cyber incident reporting framework that enables the sharing of aggregated data, anonymised to protect sensitive information, so that insurers and reinsurers can develop adequate pricing and risk management models."

Fausto Parente, Executive Director of EIOPA, 2020

Managing modelling and data risks

Key risks

- Stress test scenarios have shown the materiality of cyber risk, with potential losses comparable to large national catastrophe (NatCat) events. However, there is significant divergence in modelling methodologies and assumptions among firms.
- Our research suggests that firms currently rely heavily on subjective expert judgment, leading to inconsistent risk assessment models across the industry.
- Poorly understood or changing correlations due to lack of incident data can translate into inaccurate or inadequate estimations of capital, pricing and projected losses.
- Creating and embedding appropriate feedback processes to enhance data gathering and understanding is challenging as cyber risks evolve quickly over time – feedback therefore needs to flow quickly and frequently around the organisation and to the board, in order, for example, to support decision-making with up-to-date information and enable monitoring of risk profile.
- Cyber models are still developing, and require substantial resources to populate, run and challenge. Where firms use external models, they often have limited visibility of the underlying data, assumptions and calculation methodologies.
- Given some of the challenges and current limitations of modelling cyber risk, robust model validation is critical for the board (and the firm's supervisors) to have confidence in cyber models. Models used to understand cyber risk may require more frequent reviews and more intensive and searching validation than other more established models.

Actions for firms

- Supervisors will expect firms to show they are taking steps to reduce existing uncertainties in modelling cyber risks, and insurers should be prepared to explain and document the validity of their approach.
- While the usual model risk management (MRM) principles apply, firms need to pay particular attention to the implementation of their MRM frameworks for their cyber models, in particular model validation, if they are to build supervisory confidence in their ability to manage cyber risks.
- In order to make the best use of limited expert resources for a peril that affects multiple lines of business, careful design and implementation will be required for cyber models, especially where firms rely more heavily on legacy systems or manual processes.
- Supervisors consider some data sharing should help the market develop its modelling capabilities. Firms may be reluctant to share proprietary data. However, there may be some clear positive-sum solutions, such as using Information Sharing and Analysis Centres to collect cyber incident data. In our view, improving data collection and use capabilities should be a key priority for firms.

Managing modelling and data risks

Positive supervisory indicators

- Processes have been put in place to ensure cyber risk modelling is – and remains – fit for purpose. This could include using back-testing, severe but realistic stress test scenarios, and external vendor models to challenge in-house views.
- Subjective model judgments are clearly documented, and challenged at regular intervals to ensure they remain valid and still fit the firms' cyber risk appetite.
- The insurer conducts ad-hoc deep dives on e.g. whether the claims function captured cyber-related events, as back-testing will only be effective if events are captured and documented appropriately as and when they occur.
- A data organisation approach has been developed and agreed by the board, ensuring consistent use of data in-house, and is implemented across different classes of business. This may involve the development of a cyber risk taxonomy that events can be tagged against.
- There is a process in place to capture cyber risk exposure information in order to produce aggregation reports and, over time, identify segmentation characteristics that affect correlations between e.g. sectors or geographies. This, in turn, will help boards adapt their cyber risk appetite.
- The insurer has documented material cyber models in its model inventory and can explain how its model risk management framework has been applied for each of those models, including where key judgments have been made.

Negative supervisory indicators

- There is no single view of cyber terminology across the firm. Different classes of business underwriters use different words in contracts to mean the same thing, or similar words that are understood to mean different things.
- Cyber claims MI is collected at irregular intervals or on an ad hoc basis, and/or relies on informal processes.
- Specificities of cyber risk models are not taken into account in model lifecycle management, for example new or complex modelling approaches are not matched by more frequent reviews and/or validation. Validation focuses on process compliance rather than qualitative assessment.
- Subjective assumptions are not challenged in sufficient depth by the board, and/or rely on the expertise of too few people. The board is unable to point to evidence of challenge to subjective assumptions.
- Stress test scenarios do not reflect the appropriate calibration standards and/or are not severe enough. The firm is unable to justify why the scenario(s) used is/are adequate.
- Board members tend to rely solely on members of the board or senior management who are seen as cyber specialists when discussing and making decisions on cyber risk issues.

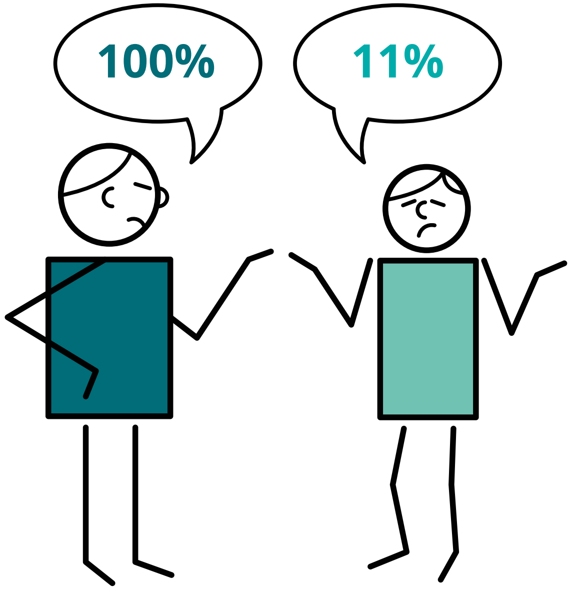
Managing modelling and data risks

"With correlation, once you get a grip on how different policies interact, it becomes easier to manage. Every now and then you will have to tweak your models with new data, but they will become more understandable over time."

Interview with cyber underwriter, 2020

A lack of accurate information on cyber risks will undermine the quality of MI, and in turn the key governance processes that it supports (such as quarterly reviews of cyber exposures by the board). We expect supervisors to be alert to any signs that governance processes are simply 'going through the motions', or that indicate lack of confidence in MI and data. Firms should be able to demonstrate the validity of MI that goes to the board, while continuing to challenge it appropriately and understand its limitations, especially for what supervisors see as a widely misunderstood risk.

Lost revenue percentages range used to assess business interruption costs



Source: Bank of England IST 2019.

"Incident breach data is probably not used as much as it could be."

Interview with cyber insurance carrier incident responder, 2020

Managing modelling and data risks

"Du fait d'un faible historique de sinistralité, il n'existe pas à ce jour de base statistiques fiables, alimentées par des données homogènes et répertoriées selon une nomenclature stable et partagée."[2]

La distribution des garanties contre les risques cyber par les assureurs. ACPR, 2019

"Getting regular and good aggregation reports can be complicated – improving your systems is part of the issue."

Interview with cyber underwriter, 2020.

Questions for boards

- Do we have sufficient expertise as a firm to underwrite cyber risks? Where do we need to invest in order to get there?
- How should we engage with the industry and policymakers on data-sharing? How would data sharing affect our competitive position?
- What scenarios have we used to help calibrate our models? Are these realistic? Who has designed them and are they in line with the severity of regulators' stress test scenarios?
- How often are we generating aggregation reports? Do we believe this is frequent enough? What is preventing us from generating more frequent reports?
- Do we have enough cyber expertise across our functions? What operating models are we considering to develop our understanding of cyber risk across insurance lines and business functions?
- How are we evaluating the business interruption cost of a range of cyber events? Are we being to sufficiently conservative or overly pessimistic?
- What does back-testing tell us about the adequacy of our model given the fast changing nature of cyber risk? Can we be confident that it captures our cyber exposures sufficiently accurately? Do we understand where it does not?
- How frequently are we validating our models? Is that frequency in line with the fact that the risk may change quicker than for other lines of business?
- What processes have we followed to set our correlation assumptions? How much is expert-driven versus data-driven? What can we do to remove subjectivity in our assumptions over time?
- Is creating a centre of excellence for cyber risk an approach that would benefit our organisation?

[2] 'Due to low claims history, there are still no reliable databases fed by homogenous data and catalogued using stable and shared nomenclature.'

Managing modelling and data risks

"Should the European legislation consider that cyber-insurance is a distinct class of insurance, which would need to be subject to its own authorisation process by public authorities?"

Public Consultation on review of prudential rules for insurance & reinsurance firms (Solvency II Directive). European Commission, 2020

"We built our own internal models and use external providers to form a hybrid view. A lot of insurers are licencing external actors. Insurers are buying reinsurance on the back of models they can't fully validate."

Interview with cyber underwriter. 2020

Checklist for boards

- ✓ Develop a strategy and systems that will enable appropriate MI from different lines of business and feedback loops between different functions.
- ✓ Adapt model risk management control processes and disciplines to cyber risk – including shorter model validation cycles.
- ✓ Understand the effect of limited data availability for cyber risk modelling, and decide on an approach to mitigate potential risks and reduce them over time.
- ✓ Develop risk appetites for cyber risk underwriting, embed these using lower-level controls, and revisit them as the firm's knowledge on cyber risks increase – or when new or previously unknown correlations between e.g. industries emerge.
- ✓ Consider the best way to make use of limited cyber underwriting expertise, for example by creating a centre of excellence. Review the available knowledge and expertise on cyber risk issues across all three lines of defense, including the internal audit and validation functions.
- ✓ Consider whether cyber risk is given the appropriate focus in the ORSA.

Managing tail risks

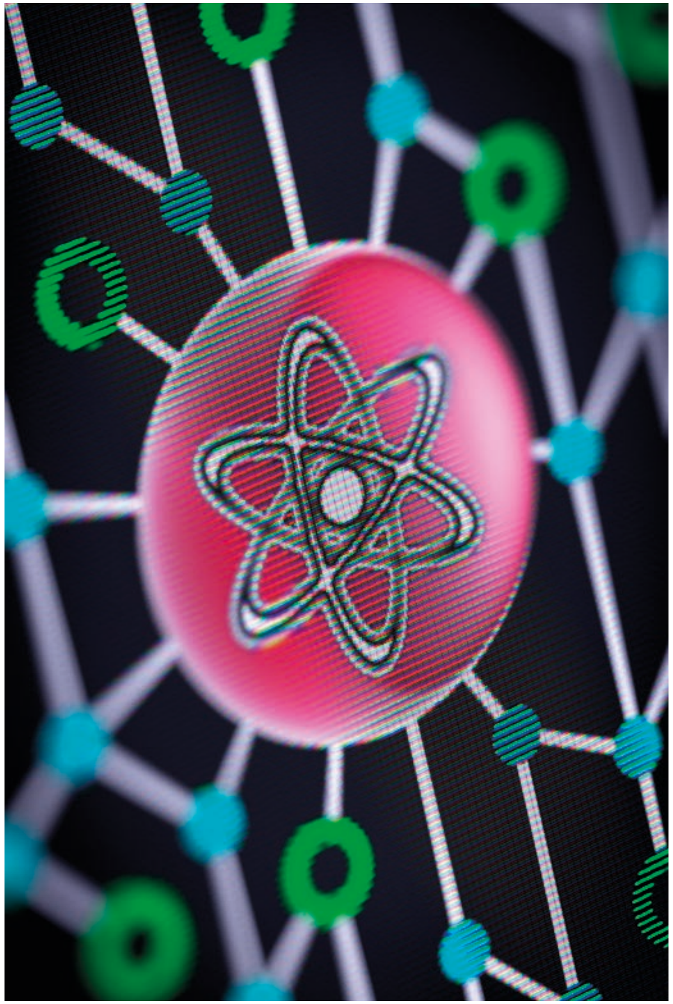
"Further research is desirable to explore, when applicable, the possible solutions to address potential systemic cyber risks and to evaluate the potential for aligning extreme event risk sharing platforms across perils."

EIOPA Strategy On Cyber Underwriting, 2020

- Cyber tail exposures are potentially very significant, exacerbating the challenges we have already identified in this report, including potential exposures to silent cyber risk and the lack of available data, as well as immaturity of some models. Comprehensive risk mitigation programmes for cyber underwriting risk with appropriate management actions are therefore crucial.
- While methods exist to manage and mitigate tail cyber risks, such as reinsurance and insurance-linked securities (ILSs), these are not as developed in terms of capacity as in other lines of business such as NatCat risks.
- Public backstops currently exist for some types of extreme risks (e.g. nuclear), and the COVID-19 pandemic has added weight to discussions on whether government should assume responsibility for further types of extreme "contingent liabilities". Some regulators have floated the idea that such backstop arrangements may be appropriate for the most extreme cyber events, but very compelling evidence would likely be required that the risks cannot be managed economically by the private sector.

"The systemic nature of major potential events is another type of external challenge which makes it very difficult to understand the dimension and the accumulated risks for the market as whole."

Understanding cyber insurance – A structured dialogue with insurance companies. EIOPA, 2018



Managing tail risks

Key risks

- Potential for extreme cyber events and higher correlations mean that risk transfer and diversification is critical for cyber risks.
- Firms that do not have a good understanding of their cyber risk exposures may inadvertently retain more risk than their risk appetite allows. This is especially true for silent cyber risk exposures.
- There is also uncertainty around how different types of reinsurance contracts will respond to silent cyber risks, potentially leaving the insurer liable for larger losses than anticipated.
- Given the lack of historical data, insurers need to rely on realistic disaster scenarios that have not been experienced in reality, adapted to their own risk profile, to understand accumulation risks.
- Insurers looking to diversify away from reinsurance may need to consider potential constraints on the availability of alternative risk transfer mechanisms. For example, correlations between cyber risk and market risk may limit appetite for cyber risk to be transferred to capital markets through ILS, in comparison to natural catastrophes.

Actions for firms

- Insurers may need to perform a bottom-up review of existing reinsurance programmes to ensure appropriate coverage of different types, and sizes, of cyber risks.
- In order to avoid a reinsurance programme that does not respond appropriately to the insurer's risks, e.g. one that retains correlated risks while transferring uncorrelated risks, firms with large cyber exposures will have to perform extensive model back-testing and validation, and consider the results when designing reinsurance strategies that fit their overall cyber risk appetites.
- A lack of capacity for reinsurance and/or other risk transfer mechanisms may be compounded by the fact that reinsurers are sometimes given limited amounts of information about the risks ceded to them. Provision of more information on cyber risk exposures by primary insurers may be necessary to unlock more reinsurance and other risk transfer capacity.

"The systemic nature of major potential events is another type of external challenge which makes it very difficult to understand the dimension and the accumulated risks for the market as whole."

Understanding cyber insurance – A structured dialogue with insurance companies. EIOPA, 2018

Managing tail risks

Positive supervisory indicators

- ⊕ The insurer has conducted a board-led deep dive into reinsurance arrangements to understand whether the contract wording matches the cyber exposure that is believed to be ceded.
- ⊕ Reinsurance strategies are revised in line with risk appetites and model validation cycles, for example to reflect newly understood exposures.
- ⊕ Board MI for cyber underwriting risk contains stress tests that explicitly consider the potential for loss aggregation at extreme return periods.
- ⊕ The primary insurer puts effort into providing information to reinsurers about the types of risks ceded, facilitating further risk transfers to, for example, capital markets.
- ⊕ The insurer has used scenario analysis to develop management actions to be applied in case of an extreme cyber event.
- ⊕ The board and senior management understand what types of reinsurance are needed for different types of cyber risks and events, and the reinsurance programme is adjusted accordingly.

Negative supervisory indicators

- ⊖ Cyber stress test results are not taken into account in the firm’s overall risk appetite and not appropriately used in board decision making.
- ⊖ There is no review of the risk mitigation programme in view of evolving affirmative and non-affirmative cyber risk exposures.
- ⊖ The board is overly confident about its cyber risk reinsurance arrangements, and the status quo does not appear to be challenged.
- ⊖ There is no understanding as to how different reinsurance programmes to cover peak and accumulation risks will affect the capital management strategy.
- ⊖ The insurer does not consider risks posed by its reinsurance programme, for example concentration risks.

> *“Cyber is an aggregating class. Even at the low end, ransomware can trigger multiple policies.”*

Interview with cyber underwriter, 2020

Managing tail risks

"It is important to enhance the use of scenario analysis to assess accumulation risk for insurers."

EIOPA Workshop on Cyber Insurance, 2019

Questions for boards

- Are we confident that our existing reinsurance and other risk mitigation programmes adequately capture risks that we do not wish to retain?
- What different types of risk mitigation techniques should we use to manage peak and accumulation cyber risk?
- What is the capital, and overall, trade-off between purchasing reinsurance and maintaining insurance risk but using alternative mitigation techniques such as lower limits?
- How are we ensuring that our stress tests are severe enough to reflect a 1-in-200 (or greater) return period?
- How did we get to the 1-in-200 year event scenario? How have we reflected the uncertainty associated with our risk exposures into our model assumptions, scenarios and calibrations?
- Have our model assumptions, scenarios and calibrations been subject to qualitative challenge from the validation function?
- Are we confident that the validation function has sufficient expertise and knowledge to apply such challenge?
- Should we be working with the industry and other stakeholders to identify creative risk mitigation solutions to extreme risk issues?
- Can barriers towards further risk transfer to capital markets be overcome through more collaboration?

Managing tail risks

"Currently, reinsurance rates are quite cheap – but there is not a lot of capacity."

Interview with cyber insurance underwriter, 2020

Checklist for boards

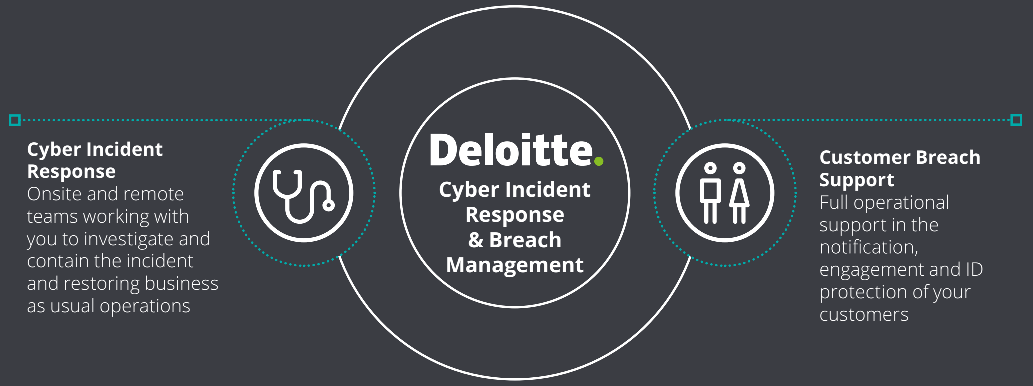
- ✓ Ensure reinsurance arrangements reflect cyber exposures and that the wording is understood and robust.
- ✓ Challenge the severity – too much but also too little – and realism of scenarios used to test accumulation and extreme risks.
- ✓ Engage with the different risk mitigation techniques available and weigh their most effective use, based on the specific shape of the portfolio of cyber risk exposures.
- ✓ Decide on a set of management actions to be taken in the case of a severe cyber event.
- ✓ Review risk transfer strategies at regular intervals, to identify whether an improved understanding of the risk requires the risk transfer programme to be updated, or creates new opportunities such as transferring larger portions of the risk to capital markets.
- ✓ Ensure reinsurers have sufficient information to make appropriate judgements on the risks transferred to them.

How Deloitte can help

As cyber threats evolve and become more complex, many business leaders recognise they cannot manage the challenge alone. The threats are constantly evolving and increasing in volume, intensity and complexity. Cyber Incident Response & Breach Management has therefore become a major focus for business leaders and boards. It has become more likely that an attack can penetrate an organisation's defences and security controls. When this happens, organisations must respond quickly, thoroughly and decisively.

How can Deloitte support your organisation?
As soon as an attack happens, our specialist teams will be deployed into your organisation to:

- Quickly understand the nature of the incident to help answer and address the questions of what, where and how
- Effectively contain the security incident, breach or attack
- Minimise the impact associated with data loss in terms of the cost of time, resources and diminished customer confidence
- Provide guaranteed capacity to notify, support and protect your customers at speed – providing you with peace of mind and protection for your brand and reputation
- Introduce a heightened level of management and controls that can strengthen your IT and business processes, helping your business focus on core activities that deliver value for the organisation



Cyber Incident Response
Onsite and remote teams working with you to investigate and contain the incident and restoring business as usual operations

Deloitte.
Cyber Incident Response & Breach Management

Customer Breach Support
Full operational support in the notification, engagement and ID protection of your customers

Technology to the rescue!
With the ever growing use of AI (Artificial Intelligence), there are many ways to help firms understand risks hidden in policy wordings of old. One such company working on this is RiskGenius. Recently, policy wording has been brought to the forefront of people's minds. The reality is we have been looking for a better way to deal with these for years.

As an example, for COVID-19:

- Property policies that do not explicitly exclude viruses, and are read to satisfy the "physical damage or loss" requirement, may create liability.
- In the coming months casualty policies could be triggered by a host of litigation, involving negligence, D&O claims, and other related suits stemming from COVID-19.
- Market bodies, regulators, governments and US insurance commissioners are already questioning insurance firms regarding COVID-19 coverage issues.

This has raised challenges world over from a legislation perspective, including:

- Exposures will vary by jurisdiction. Governments are already moving to introduce legislation requiring firms to pay out for COVID-19 claims where policyholders would not otherwise be covered.
- US legislatures have issued statements determining property damage to trigger claims under Business Interruption policies.
- The UK Treasury Committee has written to the ABI asking whether the industry would be flexible over Business Interruption.
- Questions have been raised in the UK House of Commons as to whether the Government would require insurance companies to define COVID-19 as a specified notifiable disease for the purposes of claims made by businesses affected by the Government's order to close.

For Silent Cyber, the same challenges relating to exposure prediction, understanding wordings identifying emerging risks all ring true. Machine reading these policies provides a fast, accurate way to understand the actual exposure. RiskGenius can analyse thousands of data points across hundreds or thousands of insurance policies, giving you a detailed insight on your specific risk exposure. Click here to consult the RiskGenius Silent Cyber guide

Bibliography

- Rapport Annuel. ACPR, 2018
- La distribution des garanties contre les risques cyber par les assureurs. ACPR, 2019
- Speech by Felix Hufeld, President of the Federal Financial Supervisory Authority (BaFin), at the 12th Annual Bermuda International Regulatory Forum. BaFIN, 2019
- Supervisory Programme: Insurance Supervision. BaFin, 2020
- Future of Finance Report. Bank of England, 2019
- The Bank of England’s response to the van Steenis review on the Future of Finance. Bank of England, 2019
- A Fundamental Approach to Cyber Risk Analysis. Boehme et al., 2018
- Cyber Exposure Data Schema V1.0. Cambridge Centre for Risk Studies, 2016
- Managing Cyber Insurance Accumulation Risk. Cambridge Centre for Risk Studies, 2016
- Speech by Sylvia Cronin, Director of Insurance supervision, on “going digital and remaining safe”. Central Bank of Ireland, 2018
- Demystifying cyber insurance coverage. Deloitte Center for Financial Services, 2017
- Model Risk Management – Building supervisory confidence. Centre for Regulatory Strategy, 2018
- Understanding Cyber Insurance – A structured dialogue with insurance companies. EIOPA, 2018
- Summary of Workshop on Cyber Insurance. EIOPA, 2019
- Speech by Gabriel Bernardino, Chairman, EIOPA, at the 3rd Annual FinTech and Regulation Conference. EIOPA, 2019
- Speech by Gabriel Bernardino, Chairman, EIOPA, at EIOPA workshop on cyber insurance. EIOPA, 2019
- Cyber risks for insurers – challenges and opportunities. EIOPA, 2019
- Financial Stability Report – June 2019. EIOPA, 2019
- Cyber insurance market working group – Summary Report. EIOPA, 2020
- Strategy on cyber underwriting. EIOPA, 2020
- Speech by Fausto Parente, Executive Director, EIOPA, on cyber underwriting: managing the risks from digital finance. EIOPA, 2020
- Commonality of risk assessment language in cyber insurance – Recommendations on Cyber Insurance. ENISA, 2017
- Public Consultation on review of prudential rules for insurance & reinsurance firms (Solvency II Directive). European Commission, 2020
- Advancing Accumulation Risk Management in Cyber Insurance . Geneva Association, 2018
- Extreme cyber risks and the non-diversification trap. Martin Eling, Werner Schnell, 2017
- Advancing Cyber Risk Insurance Underwriting Model Risk Management beyond VaR to Pre-empt and Prevent the Forthcoming Global Cyber Insurance Crisis. National Association of Insurance Commissioners Expert Paper, 2017
- Enhancing the Role of Insurance in Cyber Risk Management. OECD, 2017
- Dear CEO letter from Chris Moulder, director, general insurance, on Cyber Underwriting Risk. PRA, 2016
- Cyber insurance underwriting risk Consultation Paper 39/16. PRA, 2016
- Cyber insurance underwriting risk Policy Statement 15/17. PRA, 2017
- Cyber insurance underwriting risk Supervisory Statement 4/17. PRA, 2017
- Dear CEO letter from Anna Sweeney, director, insurance supervision, on Cyber Underwriting Risk: follow up from survey results. PRA, 2019
- General Insurance Stress Test 2019 – Scenario Specification, Guidelines and Instructions. PRA, 2019
- Speech by Charlotte Gerken, Director, Cross-Cutting and Insurance Policy, on Insurance risk management in a changing world. PRA, 2019
- Dear CEO letter from Anna Sweeney, director, insurance supervision, on Insurance Stress Test 2019 and Covid-19 stress testing: feedback for general and life insurers. PRA, 2020
- Petya cyber industry loss passes $3bn driven by Merck & silent cyber. Reinsurance news, 2018

Contacts

Andrew Bulley
Partner, Risk Advisory
EMEA Centre for Regulatory Strategy
+44 20 7303 8760
abulley@deloitte.co.uk

Henry Jupe
Director, Risk Advisory
EMEA Centre for Regulatory Strategy
+44 20 7303 8972
hjupe@deloitte.co.uk

Linda Hedqvist
Manager, Risk Advisory
EMEA Centre for Regulatory Strategy
+44 20 7007 7333
lhedqvist@deloitte.co.uk

Quentin Mosseray
Assistant Manager, Risk Advisory
EMEA Centre for Regulatory Strategy
+44 20 7007 7333
qmosseray@deloitte.co.uk

Nigel Walsh
Partner, Consulting
Technology Transformation | InsurTech
+44 20 7303 8586
ndwalsh@deloitte.co.uk

Mark Whitehead
Director, Risk Advisory
Customer Breach Support
+44 20 7303 0698
marwhitehead@deloitte.co.uk

Download a digital copy of this report, and others like it, at Deloitte.co.uk/ECRS

CENTRE *for*
REGULATORY STRATEGY
EMEA

The Deloitte Centre for Regulatory Srategy is a powerful resource of information and insight, designed to assist financial institutions manage the complexity and convergence of rapidly increasing new regulation.

With regional hubs in the Americas, Asia Pacific and EMEA, the Centre combines the strength of Deloitte's regional and international network of experienced risk, regulatory, and industry professionals – including a deep roster of former regulators, industry specialists, and business advisers – with a rich understanding of the impact of regulations on business models and strategy.

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Designed and produced by 368 at Deloitte. J19936