Practical Management of Cyber Exposures and Aggregations

Exposure Management Cyber Working Group

lloyd's market association

Acknowledgements

This paper has benefitted significantly from inputs and comments from the members of the LMA Exposure Management Working Group.

Special thanks go to:

Laura Freeman
Apollo

Michelle Gascoin
W/R/B Underwriting

Sanjiv Sharma
LMA

Lauren Restell
Lloyd's

Joanna Fairbairn
CNA Hardy

James Simpson
Blenheim

Rosie Pepys
Talbot

Ashley Kent
Envelop Risk

William Hale
QBE

We would also like to thank key reviewers throughout this process, including:

Emma Watkins
Lloyd's

Samantha Dickens
Lloyd's

Lloyd's Market Association's Cyber Risk Strategy Group

While we are grateful for the input provided by the individuals listed above, we wish to make clear that this paper is the work of the authors and nothing in this paper should be taken as expressing the view of any of the individuals mentioned or the organisations they represent.

Contents

The Lloyd’s Market Association (LMA) disclaimer

Foreword

I am pleased to introduce this report on the practical management of cyber exposures and aggregations. Cyber risk has emerged as a pivotal challenge in the industry landscape and beyond, characterised by its dynamic, systemic and global nature. The rapid evolution of technology, in particular the recent advancements in artificial intelligence, and the increasing interconnectivity of systems have created unique complexities for governments, corporations and individuals.

This report highlights the key issues in managing cyber risk today, including the challenges of data quality and governance, the evolution of exposure management frameworks and the role of cyber aggregation frameworks and models. It explores the benefits and drawbacks of various modelling methodologies and emphasises the need for upskilling within exposure management teams.

Lloyd's has been actively engaged in addressing these challenges through its Cyber Market Management Strategy. This strategy is built around four pillars: assessing capability, understanding exposure, preparing for major events and developing insights and market intelligence, aiming to ensure a thriving and sustainable cyber insurance market. It underscores the critical need for the industry to work collaboratively to embed cyber exposure management best practices.

I trust this report will serve as a valuable resource for the market as we seek to navigate the complexities of cyber risk management. I would like to thank the LMA Exposure Management Working Group members and Lloyd's representatives who authored and reviewed this report, sharing their experience, insights and expertise for the benefit of our market.

Sanjiv Sharma
Head of Actuarial & Exposure Management
Lloyd's Market Association

Executive summary

This paper has been produced by the LMA Exposure Management Cyber Working Group to complement the LMA Cyber Risk Strategy Group's Scoping Out Systemic Cyber Risk framework.

Cyber risk has emerged as one of the most dynamic and challenging perils in today's risk landscape. It is a human-caused and often maliciously motivated threat that can transcend geographical and sectoral boundaries, creating unique challenges for insurers and reinsurers. Unlike 'traditional' perils, cyber events are not easily constrained by time, space or rational progression, complicating efforts to assess exposure, manage accumulations and define events. Rapid evolution of technology, diverse threat actors and growing interconnectivity exacerbate this complexity, demanding a multidisciplinary approach to risk quantification and management. This report highlights the key issues in managing cyber risk today, including data quality and governance. It discusses the evolution of exposure management frameworks and the role of cyber aggregation frameworks and models in creating a more structured understanding of accumulation potential.

This report also explores the challenges of collecting and standardising data, the benefits and drawbacks of various modelling methodologies and the need for upskilling within exposure management teams.

Additionally, the evolving regulatory landscape, including *Lloyd's Principles for Doing Business and Best Practices for Managing Non-natural Catastrophe Risk*, as well as the PRA's Supervisory Statement SS4/17 on Cyber Insurance Underwriting Risk, Lloyd's COBRA assessment and Lloyd's Cyber Strategy all underscore the critical need for the industry to adapt to this emerging peril with rigour, agility and innovation.

While the management of cyber risk accumulations is a relatively new discipline, we are well equipped to face the challenges discussed in this document, providing that we work to ensure complete, accurate and timely data collection and storage – a crucial factor, as with all exposure management practices. Standardised 'primary' cyber characteristics that are routinely disclosed and captured will go a long way towards ensuring that cyber exposure management practices become embedded into syndicates' exposure monitoring.

Ongoing Lloyd's workstreams aimed at managing cyber risk

Cyber Strategy Pillars

The Cyber Market Management Strategy was shared in June 2024 with the aim of contributing to a thriving, sustainable market and to ensuring that all market participants maintain appropriate expertise to manage Cyber risk in a rapidly evolving landscape. The strategy incorporates four pillars:

Pillar 1: Assessing capability to ensure growth is commensurate with underwriting capability.

Pillar 2: Understanding exposure to ensure managing agencies have the three key perspectives to appropriately manage the risk: data, scenarios and probabilistic models.

Pillar 3: Preparing for a major event to ensure managing agencies are not caught off guard.

Pillar 4: Developing insights and market intelligence so that Lloyd's is the best in class for cyber.

Cyber strategy implementation

Pillar 1: Assessing capability

Lloyd's has developed a framework (COBRA) designed to ensure that syndicates writing material amounts of cyber business have appropriate cyber capabilities. This includes appropriate skills, tools and controls. The framework reviews syndicate approaches to cyber insurance across three principles-based oversight (PBO) dimensions: underwriting (including pricing), non-natural catastrophe exposure and capital. This aids the management of the diversification of risk across portfolios.

Executive summary continued

Pillar 2: Understanding exposure

This pillar seeks to improve Lloyd's understanding of market risk as well as opportunity within the market.

At the start of 2025, Lloyd's requested aggregates for cyber to understand the exposure in the market by industry, geography and company revenue. From this Lloyd's aims to understand more about exposure as well as the level of diversification of the market.

Linked to this, there is a planned refresh of the Cyber Realistic Disaster Scenarios (RDS). This refresh will ensure that the scenarios are fit for purpose and align with the current risk landscape.

The Lloyd's ABI Cyber Working Group authored a publication entitled '*Components of a major cyber event: a (re)insurance approach*'. This presented a shared market view of the major components of an event in a simplified framework. A better understanding of Lloyd's cyber exposure enables better risk control.

Pillar 3: Preparing for a major event

A major catastrophe event has not been experienced in cyber, unlike in other classes. For this reason, Lloyd's wants to ensure that should a major catastrophe event happen, the market is prepared to respond and is ready for the impacts that follow. In doing so, Lloyd's aims to assess the response of third-party contracts for the supply of incident response. As well as this, Lloyd's is in the process of adopting a more granular claims data framework for cyber. Throughout the Cyber Market Management Strategy, Lloyd's has been working alongside the government to understand priorities.

Pillar 4: Developing insights and market intelligence

This element of the cyber strategy aims to reassure the market that Lloyd's is at the forefront of cyber developments and will continue to be a thriving marketplace for cyber insurance. This has involved, collaboration with the broader Lloyd's ecosystem, including brokers, on innovation. Cyber innovation has been showcased through the Lloyd's Lab Accelerator program. In addition to this, Lloyd's has continued to deliver high quality events and publications on the topic. This includes work by Lloyd's Futureset as well as events with partners like Sasig. For this technical topic, Lloyd's has also worked with the market to facilitate the upskilling of professionals in the market.

Introduction to cyber risk, challenges and uncertainties

Introduction to cyber risk, challenges and uncertainties

Cyber is an emerging, dynamic and man-made risk, with origins that are often, but not always, malicious. This presents new challenges in ascertaining accumulation potential or defining events.

Cyber risk is a distinct and relatively new set of perils. Furthermore, these perils can have significant impacts on those affected and have the potential to spread widely, affecting large numbers of people across geographical boundaries and potentially impacting the ability of states to function. These events can lack a clear beginning, end or rational progression as they spread from one system to another. The outcomes of cyber events greatly depend on the quality of the defence, response and recovery measures organisations have in place, and human actions. Different cyber events can also vary widely in their likelihood of causing major operational disturbance, property damage or, potentially, loss of life.

Challenges

With the uncertainty that comes with defining and then managing a cyber threat, ensuring consistent reporting, pricing adequacy, model validation and completeness and governance is challenging. Until recent years, cyber exposure management was often managed exclusively by underwriters and actuarial teams. This responsibility is now often being brought under the remit of exposure management teams.

Exposure management teams are familiar with probabilistic natural catastrophe models within exposure management frameworks, and non-natural catastrophe classes are now expected to have similar levels of controls.

- As exposure management teams take more responsibility for centrally managing these risks, it is important that investment is made in this discipline.
- There are a variety of different datapoints being collected across the market, from several different data sources. While this helps to ensure data is as complete as possible, there is not currently a single standardised data schema being used, resulting in further challenges.
- There are many vendors now offering models to manage syndicates' cyber risk. While choice of vendors is beneficial, challenges exist in selecting the most appropriate provider.

Data sources

Data sources

While the quality of exposure data used for cyber insurance and reinsurance has been improving in recent years, it still lags behind more established classes of business. This issue has begun to be addressed by the introduction of Lloyd's minimum data requirements for cyber insurance.

Data quality and availability are key factors when determining which aggregation methodology to use. Key areas to consider include consistency, completeness and accuracy. While to some degree the quality of the data companies receive is something they cannot fully control, the way in which the available data is incorporated into any analysis can be carefully reviewed and implemented. It is also incumbent upon insurers and reinsurers to request pertinent information in order to gradually improve the data available.

Exposure managers experience a variety of challenges associated with collecting accurate, appropriate and complete cyber data. This paper explores some of those challenges and suggests some practical approaches to overcoming or mitigating their impacts.

Understanding important data points for identifying cyber accumulations and managing exposures

Prior to the introduction of natural catastrophe models, exposure managers dealt with the same challenge of trying to identify and collect 'relevant' data fields to enable an accurate representation of exposure and to identify potential accumulations. The introduction of catastrophe models helped to standardise data fields, by defining the downstream use of this data.

The cyber market now faces the same challenge. In the absence of a single standardised data schema, a variety of fields are being collected by different entities and the cross section is not entirely consistent.

There are, however, some publicly available data schemas that syndicates can apply to their cyber exposures:

- Open Data Standards (ODS)
- Cambridge Centre for Risk Studies
- Lloyd's cyber and liability minimum data standards, published in 2020 and including the following fields:
  - Industry, e.g. a code or sector description.
  - Size of company, e.g. revenue, profit and/or number of employees.
  - Legal jurisdiction, e.g. state or country.
  - Insured Company Identifier (where possible), e.g. name, DUNS (or similar) code.
  - Defence costs, e.g. inside/outside limits or not covered.

Lloyd's undertook work in 2024 to define what is meant by cyber accumulation and to decide on important data parameters to include in a market-wide cyber aggregation data collection. The following questions were considered when developing the data collection, in conjunction with market and vendor feedback:

- What level of firmographic and technographic detail is required for understanding cyber exposure?
- If a policy covers multiple zones (be that geography, industry or revenue), where would you attribute this information to?
- What level of granularity of industry code (NAICS) is appropriate in order to contextualise high accumulation points, yet rationalising the size of data collection and ensuring consistent data collection?

Data sources continued

- Will it constitute a significant technical challenge to assign insureds or policy limits to zones?
- Would this data be easily available for direct and reinsurance?
- For portfolios where underwriting is delegated (e.g. binders), are these exposures known in this level of detail?

The pertinent fields were defined as:

- geographic area
- industry
- revenue band
- number of policies
- total aggregate of full limits
- total aggregate of sub-limits (split into direct BI, CBI (IT), CBI (non-IT) and cyber physical (CZ)).

Receiving and storing complete datasets

Cyber data challenges vary depending on the type of business or placement method. A syndicate has more flexibility to define the data required to write a policy if the business is open market. If data is being provided by a third party through a delegated authority, facility or broker arrangement, it is more difficult to define and receive data consistently at the same granularity.

Syndicates should fully understand the data they receive, identify where there are deficiencies and consider ways to mitigate these. This could be through data augmentation using commercially available third-party datasets, or by applying well-documented and considered expert judgements and assumptions where necessary. There may also be collaborative work that can be done as a wider market around coverholder data standards, for example (which will be considered as part of the 2025 Exposure Management Delegated Authority deep-dive project). Regardless of the approach, data quality and limitations should be explicit, regularly reported and monitored, and a plan should be put in place to make improvements over time.

It is imperative to store cyber exposure and policy data in an easily accessible place, as a ‘single version of the truth’ for any downstream use. If exposures and policy information are stored in separate software, there needs to be regular reconciliation and data consistency checks performed to ensure that live cyber exposures from both cyber and non-cyber policies with cyber exposure are considered in portfolio management and in comparisons against risk appetites.

Receiving timely data

Data delivery timeframes can range depending on the placement method. There can be a time lag on receipt of delegated and facilities bordereaux. Inwards reinsurance data can also be outdated or provided with a time lag. These occurrences and limitations should be fully understood and appropriately mitigated. This might include simply requesting more frequent data from the data provider, working with the data provider to facilitate the data and improved data cadence going forwards (making the digital exchange easier). Alternatively, it could consist of augmenting the in-force data with synthetic data or a rolled-forward portfolio to ensure a complete dataset is available for downstream decision making at any given time.

Dealing with legacy exposure data

There are also some policies with trigger types that are still subject to potential latency claims (i.e. risks attaching during) and where the policy data has not been digitised or is not immediately accessible for the purposes of exposure management. This can be problematic with reporting structures and although policy coverages have evolved, this has generally been post-event, so managing this data type in a timely and accurate manner is challenging.

Clearly documented and managed assumptions can be applied to datasets to account for this data in exposure and aggregation management, to ensure that it is not omitted.

Data sources continued

Data governance, reporting and progressive improvement

Improving cyber exposure data over time must be supported by robust data governance. Data can only be effectively improved if there are ways to measure, report and monitor cyber data accuracy, appropriateness and completeness over time. There should be clear responsibilities and ownership of these metrics, as well as plans put in place to continually improve them, all of which can be tracked.

It is important for managing agencies to understand the sensitivities around applying mitigative approaches to downstream decision making. This is especially important where a data parameter might be particularly sensitive. Documenting adjustments and expert judgements and their sensitivities helps to control this effectively. It also helps to prioritise and manage any future updates or data changes required.

Decision makers should be aware of how the data supporting the downstream analysis might have impacted the outputs they are using. A summary of data quality, limitations and mitigative approaches put in place should be available to them.

Cyber models

Cyber models

Cyber is a relatively new and distinct peril. Unlike more traditional risks, cyber does not benefit from extensive historical datasets or well-defined physical parameters. For instance, natural catastrophes like hurricanes are constrained by known limits – a hurricane cannot exceed category 5 on the Saffir-Simpson scale, for example. In contrast, cyber threats evolve rapidly, with contentious upper bounds and unpredictable patterns, making them far more challenging to quantify and manage. This presents some challenges for Lloyd's syndicates (and more generally the insurance/reinsurance industry) in effectively managing large-scale cyber risk accumulation.

Cyber is relatively new class and is advancing quickly. As such, the need for personnel and expertise in cyber is outstripping the availability in the traditional insurance market.

In this section, we explore the current landscape of modelling methodologies available to syndicates, taking care to maintain an impartial and unbiased view of a wide range of approaches, ranging from straightforward methods to highly sophisticated modelling approaches.

Effective management of cyber accumulation risks requires not only an understanding of what each methodology offers, but importantly, the adoption of methodologies that align with a syndicate's capabilities and regulatory expectations. A syndicate with little exposure to cyber risk would not be expected to licence probabilistic models from third-party vendors, and a simple sum of aggregates may be sufficient. At the other end of the scale, a syndicate that specialises in cyber may be expected to licence an external model, supported by an internal view. Whatever approach a syndicate uses, they should ensure appropriate governance in the implementation, application and reporting of chosen approaches.

A syndicate may be able to assess how sophisticated their cyber modelling is required to be from their maturity level under the *Principles for Doing Business at Lloyd's*. However, as cyber falls under the wider category of non-natural catastrophe risk, the assessed maturity level for a syndicate that writes a considerable amount of classes – such as terrorism or liability – may not be an appropriate guide. Syndicates may be able to get further guidance on what is expected of them from their Lloyd's Exposure Management Manager.

Robust exposure management processes utilise a multifaceted approach to managing exposure of catastrophe and non-catastrophe risk. Some common tools used by exposure management teams include aggregation, application of probable maximum loss (PMLs), deterministic scenarios and fully probabilistic models. Regardless of the level of sophistication of the methods used, when viewed together it will allow the company to have a more complete view of the risk than by using each in isolation.

Cyber models continued

Aggregation and maximum exposure model

Simple risk aggregation is often the first stage in quantifying the risk, with the complexity of the aggregations depending on the quality of the data provided and the insurer's portfolio. The key focus of aggregation is understanding the level of risk within certain parameters.

Common simple approaches to the aggregation of cyber risk include collecting the following data on the insured:

- industry (SIC or NAICS can be useful)
- revenue (as a measure of size)
- domicile/jurisdiction
- number of employees.

More complex aggregation features will include data such as cloud service provider, types of software used and types of data records kept.

Attention should be focused on the level of aggregation and the number of aggregation levels/zones analysed. Aggregation at a low-level resolution will return results that are difficult to apply and quantify, whereas aggregations at too high/detailed resolution may fail to identify important correlations. Maximum exposure analysis may provide a practical and prudent method for assessing worst case potential insured losses. This approach calculates the total exposure a syndicate could face from potential attacks by summing the maximum insurance/reinsurance limits. The analysis is often segmented by key business dimensions such as geography, company size or industry sectors to provide a more detailed view of risk distribution. While it does not account for nuances such as diversification effects, it offers a starting point for understanding the upper bounds of risk. Syndicates can calculate their exposure using policy limits, providing an explainable and prudent view of accumulations that is easy to govern, without the need for complex tools or datasets (or even an understanding of the threat landscape).

Pros:

- Simple, consistent, not resource intensive to produce.

Cons:

- Overly conservative, does not accurately reflect the risk.

Deterministic modelling

Deterministic models offer a structured framework for assessing the impact of predefined cyber events. Realistic Disaster Scenarios (RDS), commonly used within the Lloyd's market, are an example of this methodology. These scenarios are typically designed by panels of external experts (although internally designed deterministic models are also commonplace) who reason about event severity, industry sectors impacted and potential financial consequences. By applying consistent assumptions across scenarios, syndicates can evaluate their portfolios' resilience to these scenarios and identify potential vulnerabilities. Deterministic models such as the Lloyd's suite of cyber RDSs provide an accessible method for stress-testing exposures against a limited set of high-impact events, with the benefit of being relatively easy to implement and audit.

Pros:

- Easy to run and to understand, provides a more accurate view of risk compared with maximum exposure.

Cons:

- Scenarios need to be reviewed regularly.
- Lack of flexibility as each scenario provides a single view of risk.

Cyber models continued

Extended ‘scenario-based’ approaches

Deterministic models offer a structured framework for assessing the impact of predefined cyber events. Some vendors like to extend this approach by incorporating a higher level of detail and sophistication in deterministic modelling. Some vendors design their deterministic scenarios by leveraging large datasets and detailed analyses of Single Points of Failure (SPoF), such as major cloud providers or widely used software services. These scenarios are structured into ‘event families’, which represent variations in how a single event could unfold and allow syndicates to explore a range of plausible outcomes for each predefined event.

Some vendors’ approaches incorporate mapping dependencies and fill gaps with data-driven estimations, providing a more complete view of systemic risks. This enables syndicates to better understand how a single event could impact industries, geographies and companies of varying sizes. The modular design of their models break scenarios into components addressing event frequency, affected footprints and severity, creating an adaptable framework for stress-testing portfolios. Scenario-based approaches like these enhance purely deterministic scenarios by incorporating dynamic variables, richer datasets and probabilistic insights, enabling a more nuanced view of systemic risk accumulation.

Pros:

- A range of scenarios provides a more nuanced view of risk.
- The vendor is responsible for keeping scenarios up to date.

Cons:

- Licences can be expensive.
- The approach is not as flexible as a fully stochastic model.

Fully stochastic modelling approaches

Stochastic models leverage probabilistic techniques to simulate thousands of potential loss scenarios, providing a forward-looking view of potential risk accumulation events. Several vendors offer proprietary stochastic models that aim to characterise and quantify the underlying threat landscape, and in doing so provide loss distributions for a wide range of cyber events. These models aim to build an understanding of the underlying system that generates the risk by probabilistically characterising the threat landscape, including threat actors, targets, attack methods, spread dynamics and motives.

This modelling approach aims to not only assess known risks, but to also uncover ‘unknown unknowns’ (in the Rumsfeldian sense), providing insight into risks that might not yet be fully understood or observed. Given this, stochastic models arguably offer a more natural and comprehensive depiction of the future systemic loss environment.

Pros:

- Licenced models from well-known vendors provide an external view, which is likely to be approved by regulators.
- Provides a range of outputs across the EP curve.
- The vendor is responsible for keeping the model up to date.

Cons:

- Licences can be expensive.
- If there is insufficient in-house expertise to fully understand the model, the results may be misapplied.

Cyber models continued

Proprietary/in-house modelling

Syndicates can choose to develop proprietary or bespoke in-house models tailored to their unique portfolios and risk appetites. These models could integrate elements of deterministic and stochastic methodologies, drawing on the expertise of in-house data science teams and threat intelligence teams. In-house models could provide the flexibility to focus on risks most relevant to a syndicate's business, allowing for customised scenarios and assumptions. They also enable syndicates to maintain control over their modelling processes, which can be advantageous for meeting specific regulatory or strategic objectives.

Proprietary modelling can also increase the agility of the team, such that changes in threat/vulnerability can be incorporated into the models. This is difficult for vendor models that have multiple clients who may or may not require the update and are limited to annual update cycles. Another advantage is that proprietary models can incorporate more detailed policy, exposure and claim data that is not available or cannot be shared by vendor models.

Pros:

- Tailor-made modelling is likely to provide the most reliable picture of accumulation risk for a syndicate's own book of business.

Cons:

- Expensive, either in consultancy fees or in the internal resources required to develop and keep the models up to date.

The landscape of cyber risk models and methodologies offers Lloyd's syndicates a broad spectrum of tools to manage large-scale risk accumulation. Ultimately, the decision on which model or methodology to adopt should reflect a syndicate's specific risk profile, regulatory obligations and strategic objectives. By understanding the strengths and applications of each approach, syndicates can effectively navigate the complexities of managing large-scale cyber risks while aligning with Lloyd's market expectations.

Lloyd’s principles

Lloyd's principles

Purpose of the Lloyd's Principles Based Oversight (PBO) framework

The Lloyd's PBO framework articulates the fundamental responsibilities expected of all managing agents in order to support the market's overall performance, capital strength and financial and reputational credibility.

The thirteen principles are outcomes focused and allow for differentiation in terms of expected maturity, according to materiality. The PBO framework is used by Lloyd's to categorise all syndicates and managing agents in terms of both their capability and performance.

Principle 2 relates directly to 'catastrophe exposure' and is further broken down into:

- Principle 2a: Natural Catastrophe.
- Principle 2b: Non-Natural Catastrophe.

This distinction recognises the overall market maturity in each of these respective exposure and catastrophe management areas.

Natural catastrophe risk-based oversight replaced the Lloyd's exposure management minimum standards in 2018 with the introduction of the Cat Risk Operational Framework (CROF), which then transitioned into PBO Principle 2a when the wider framework was deployed market-wide in 2021.

Non-natural catastrophe oversight was a new Principle (2b) for Lloyd's, and the entire market was reviewed for the first time in 2021, focusing on the most material classes.

All syndicates now have separate expected maturity and assessed maturity scores for both natural catastrophe and non-natural catastrophe. These are used to target oversight throughout the year and as part of business planning decision making.

Lloyd's Non-Natural Catastrophe Market Themes and Best Practice Paper

In 2024, Lloyd's released its *Non-Natural Catastrophe Market Themes and Best Practice paper*. The paper is a collection of insights collected from across the market as part of the initial Principle 2b, containing market themes and best practices seen across the non-natural catastrophe class landscape.

The paper is class-agnostic and focuses on some of the current best practice observed in the market. It provides practical examples that syndicates could consider undertaking in order to meet the outcomes clearly identified under each of the 10 sub-principles. In this part of the paper, we will explore examples that are directly related to cyber risk and exposure management.

It is imperative to note that these lists are not exhaustive and are intended to provide some insight into the kinds of approaches that are currently possible in the cyber space, using the outcomes framework of the Non-Natural Catastrophe Market Themes & Best Practice paper as a backdrop. There is also no explicit consideration of how expected maturity relates to these examples.

Lloyd's principles continued

Principle 2b: Practical examples to achieve cyber-specific outcomes (from an exposure management perspective)

Sub-principle 1: Cat Risk Appetites & Tolerances

Focus on: managing cyber exposure in line with agreed risk appetites and tolerances

Multi-dimensional cyber catastrophe risk appetite frameworks to avoid unforeseen accumulation risk

- Defined risk appetites and tolerances that consider the materiality of cyber within the syndicate's portfolio at a range of impacts, including extreme tail events, profit events or capital impacting events.
- Consideration of standalone cyber as a line of business and all risks policies written across other lines of business (i.e. property or casualty), which may also provide cover following a cyber event.
- Employ a mixture of risk appetites and tolerances for cyber. This may include the use of aggregate limit monitoring, use of third-party probabilistic vendor models or a suite of deterministic scenarios, which consider losses across all lines of business with cyber exposure.

Supporting syndicate-specific cyber business strategy using risk appetites

- Ensuring that cyber risk appetites and tolerances remain in line with the wider cyber strategy and business plan.
- Use of dynamic tolerances supporting risk appetites, which may reflect planned growth in a particular industry or jurisdiction.
- Syndicates demonstrate consideration to the granularity of risk appetites to enable monitoring and decision making based on current utilisations – this will differ depending on syndicate cyber materiality.

Effective use of risk appetites in decision making

- Use of underwriting guidelines to set out ownership and accountability – this can be for individuals or committees and should include a referral or escalation process to allow a flexible approach.
- Clear and regular communication of the current utilisation of cyber risk appetite metrics. Whilst there is no set template for reporting, these may encompass dashboards, checks to underwriting policy admin systems, marginal impacts etc.
- Ensuring that there is a clear process to follow (including actions and accountabilities) should an appetite be breached/near breach. This does not have to involve exclusively managing exposures down. It can also include a feedback loop to trigger a revision of current risk appetites if required by the wider business strategy.

Effective monitoring and management against risk appetites

- Use of third-party vendor models could be applicable. Alternatively, the development of deterministic scenarios and visibility of limit profiles by country, industry, sub-limits for the specific cyber coverages or jurisdiction.
- Ownership of appetites and tolerances is clear and promotes the probability of identifying a potential cyber breach before it occurs; reporting frequency supports this approach.
- Governance supports visibility across decision makers and allows performance to be reviewed and challenged appropriately.

Ensuring that risk appetites remain appropriate using feedback loops

- Defining feedback loops within the business to ensure an ongoing cycle of challenge and review of the scenarios and ensuring ongoing appropriateness and alignment with business strategy.
- Creating a synthetic cyber portfolio that reflects the upcoming Syndicate Business Forecast (SBF) year and testing planned growth or limit profile changes against the appetites in place for the coming year.
- Acknowledging that things may happen outside of this cycle, including reinsurance erosion or a real-event experience such as the recent Crowdstrike event, which may trigger review and feedback outside of a designated cycle.

Lloyd's principles continued

Sub-Principle 2: Data & Tools

Focus on: employing appropriate tools to support effective and efficient cyber exposure data capture, management and use

Managing cyber data accuracy, appropriateness and completeness

- Cyber data fields are recognised within Lloyd's minimum data requirements. Where data falls short of these standards, underwriting controls may mean that risks cannot be quoted.
- The nature of cyber means that the evolution of new data fields may be fast paced; new technologies or tools may facilitate data capture, promote data augmentation and support data quality improvements.
- Considering the use of third-party datasets to help augment deficient data where required for downstream use.
- Tracking data accuracy, appropriateness and completeness using defined metrics in regular reporting. Supporting this with defined actions for improving data where necessary, and reporting on progress against these actions to demonstrate continual improvement over time.

Managing cyber data limitations

- Documenting known cyber data limitations so that they are clear and can be considered in downstream decision making.
- Where data limitations exist, explore how existing data could be supplemented to address the limitations.
- Third-party data and recent enhancements in technology may improve data completeness.
- Where limitations in cyber data exist, consider if downstream adjustments are appropriate. Clearly documenting any adjustments made, so that it is visible to decision makers.

Using a consistent cyber view of risk and a single view of exposure for downstream decision making

- A single approach, which is considered the only 'truth' in terms of data used for onwards decision making. This may mean that certain data fields are a requirement to price and/or accept business – and that other fields can be enhanced once on risk.
- Where data quality or completeness issues are identified, an appropriate consideration of uncertainty may be applied to risk appetites or tolerances.

Supporting efficient and effective cyber exposure management with tools

- Maintain a repeatable way of capturing data, supported by data dictionaries, data validation, data quality reporting and monitoring.
- All tools used need to be appropriately tested and validated, deeming them suitable for their use case.
- View *Scoping Out Systemic Cyber Risk* paper for insights

Lloyd's principles continued

Sub-Principle 3: Exposure Monitoring & Reporting

Focus on: adoption of a robust risk-based framework for cyber exposure quantification and monitoring, to support downstream decision making

Implementing a robust, risk-based framework for cyber exposure monitoring

- How material is cyber to the syndicate? Develop a view of risk and validation process that reflects the materiality – to include an expert judgement log and underlying assumptions that can easily be updated as part of an ongoing cycle of review.
- Use of back testing and stress and scenario testing relating to cyber risk to support and articulate uncertainty and sensitivity within the portfolio.
- Embed clear responsibilities, clear feedback loops and a clear approach to governance.
- Consider how emerging risks affect cyber in the current portfolio and paired with a future iteration of the portfolio. Emerging risks need to be identified, monitored and quantified using a variety of horizon-scanning techniques.

Adopting appropriately validated cyber risk quantification methodologies

- A variety of methods to quantify cyber exposure are considered and those selected are considered the most appropriate for the syndicate's book of business.
- An appropriate view of cyber risk will be maintained by continually developing understanding of risks through active learning, development and research; an emerging risk working group may support such a framework.
- Ties back to sub-principles related to 'View of Risk Methodology' and 'View of Risk Validation'.

Regular, timely cyber reporting to support decision making

- The frequency of cyber reporting supports downstream decision making. Reporting content is developed with downstream decision makers and consumers, to ensure that the content is useful and at a sufficient level of detail. Feedback is provided as part of the governance and sign-off process and helps to shape reporting requirements over time.
- Key metrics include loss quantification by scenario, probability curves, RDS losses, utilisation against risk appetites and tolerances, data quality, data adjustments, uncertainties, sensitivities and marginal impact (where possible) with suggested actions and documented outcomes.
- Regulators are informed ahead of syndicate submissions where there are breaches of approved plan anticipated, or where returns may be submitted late.

Lloyd's principles continued

Sub-Principle 4: Resourcing & Expertise

Focus on: having the teams and expertise in place to meet cyber business needs, including strategic projects, regular deliverables and research and development

Adequate resource available to meet business needs for: 'business-as-usual' activities, research and development, reacting to real-time events, continual improvements and avoiding key person dependencies

- Performing 'business-as-usual' regular-cycle cyber quantification, reporting and providing external team support.
- Undertaking research and development to ensure continual improvement of existing cyber exposure management approaches and methodologies in light of the current and future risk landscape.
- Reacting to real-time cyber events and incorporating this experience into the existing exposure management framework.
- Formulating new and more efficient ways of delivering cyber exposure management insight to the business for both strategic and operational decision making.
- Avoiding key-person dependencies by:
  - Undertaking cross-team training and development on the latest cyber advances and development on related topics.
  - Well-documented processes and procedures that others in the team can easily use and follow.
  - Effective succession planning.

Varied team expertise

- Teams are made up of either specialists and/or generalists with a range of experience, but the team composition and skillset is appropriate in relation to the materiality of cyber (in terms of exposure from all classes) to the syndicate, ensuring appropriate resource is available.
- External expertise and resource can be leveraged where appropriate. External consultants and group-level research teams can be engaged on specific cyber topics or projects.
- Where external resource is utilised, syndicates ensure that deliverables are clear and in line with business requirements by putting in place project plans and SLAs. Syndicates ultimately own any outputs.

Lloyd's principles continued

Sub-Principle 5: Cyber View of Risk Methodology

Focus on: defining and maintaining an appropriate cyber view of risk methodology

Cyber view of risk development and outputs are robust

- Data quality sensitivities are considered and communicated along with cyber internal model inputs. This is especially important where this drives a material impact on model outputs. Deficiencies are addressed and appropriate adjustments are made and documented.
- A range of cyber quantification approaches can be utilised as internal model inputs, or as a way of providing alternative views of frequency/severity to validate internal model inputs and test sensitivity and uncertainty of the cyber view of risk.
- Approaches for generating cyber internal model inputs range from using a suite of RDSs to parameterise actuarially derived frequency-severity distributions (ranging in granularity, dependent on materiality), to the use of probabilistic outputs from third-party model vendors, which may be adjusted post-validation.
- Other experience, claims, expected loss ratios, external data sources and models are used to inform and validate the syndicate cyber view of risk methodology and assumptions.

Exposure management cyber inputs into the internal model are defined, managed, communicated and improved over time

- Expert judgements can be a significant input to cyber risk representation within internal models. Where this is the case, syndicates:
  - Maintain a comprehensive cyber expert judgement log.
  - Understand, test and communicate the sensitivities related to cyber expert judgements.
  - Clearly articulate who owns, reviews and maintains each expert judgement. Those who own the expert judgements are ultimately responsible for managing their appropriateness and use.
  - Continually seek improvements in expert judgements, as solutions and approaches to modelling cyber develop.
  - Include the use of cyber expert judgements within the in-team testing plan and critically review these as part of continuing internal model development.
- Feedback loops following real-life cyber events are used to critically test cyber representation within a syndicate internal model.

Lloyd's principles continued

Sub-Principle 6: Cyber View of Risk Validation

Focus on: implementation of an appropriate risk-based validation of the cyber view of risk, including critical review of exposure management inputs and internal model outputs used for decision making

Multiple validation points to ensure ongoing cyber view of risk appropriateness

- Additional data is used in validation, including third-party model views as an alternative view of risk, internal and externally created RDSs (i.e. an extended suite of scenarios), experience and other external sources.
- Emerging risks are considered in validating the cyber view of risk. Potential impacts of emerging risks are investigated using new scenarios, and these are used to test the cyber view of risk. An emerging risk group within a syndicate can attest to cyber view of risk completeness.

Adequate governance to critically review the cyber view of risk

- Clear ownership of the cyber view of risk and its use. Cyber view of risk is developed using subject-matter experts but is owned and managed centrally to facilitate consistent use across the business and ongoing improvement.
- Peer review and challenge provided at policy level.
- Exposure management teams participate in committees involved in the cyber view of risk sign-off process.
- All teams with specific cyber expertise feed into a critical review of the cyber view of risk through the governance framework and the findings are incorporated into future development work.

Incorporating uncertainty and sensitivities into cyber view of risk outputs

- The capital model validation process includes sensitivity and stress and scenario testing, to ensure that the cyber view of risk is reasonable and appropriate for the syndicate's portfolio.
- Where there is experience that can be used, back testing is used to help validate the cyber view of risk.
- An example approach to managing uncertainty and sensitivities would be to undertake an annual extreme sensitivity test against all cyber scenarios, to review and assess the resultant movement in capital (direction and quantum) directly associated with cyber view of risk.
- All decision makers are aware of the cyber view of risk uncertainties, sensitivities and limitations.

Lloyd's principles continued

Sub-Principle 7: Cyber View of Risk Completeness

Focus on: maintaining a materially complete representation of cyber risk in the syndicate view of risk

Clear methodology to review and test cyber model completeness

- Any areas that could impact cyber model completeness are identified, and a plan is put in place to mitigate deficiencies. The approach is clearly considered, documented so that it is repeatable, approved by relevant committees and communicated to decision makers.
- A risk-based approach is adopted, and for all material lines of business an appropriate representation of the range of potential losses, uncertainties and sensitivities is included in the cyber view of risk.

Model completeness owned and managed as part of the governance framework

- Cyber model completeness may be wrapped into the existing internal model governance process and internal model validation process, to ensure consistency in approach and Solvency II compliance.
- A consistent and joined-up approach to ensuring cyber model completeness across teams is needed. Some model completeness elements may be captured by exposure management, some by capital, some within reserve inputs or underwriting inputs and so on.

Ongoing regular review of cyber model completeness appropriateness

- Model completeness is considered and critically reviewed on an ongoing basis as part of the cyber view of risk framework. There are also triggers for review to ensure that the view of risk remains complete when changes occur to the risk profile, or with the emergence of new risks.
- The emerging risk process feeds into the syndicate's understanding of model completeness. Clear thresholds identify when an emerging risk moves from being of interest to requiring quantification and inclusion within the cyber view of risk.
- Cyber view of risk model completeness is considered in detail by capital and exposure management teams as part of validation work. It is explicitly built into the process and considers exposure management inputs into the internal model as well as completeness of the representation of risk within the internal model itself.

Consideration of future events with a forward-looking methodology

- Experience can be used to test the cyber view of risk, but potential future events (considering 'what is possible') are also included to help parameterise uncertainty and sensitivities.

Lloyd's principles continued

Sub-Principle 8: Cyber View of Risk Methodology Change

Focus on: adopting a robust risk-based framework for managing changes to cyber view of risk and exposure management methodologies: identifying, actioning, communicating and integrating these changes

Managing cyber view of risk methodology changes

- Proposed updates to the cyber view of risk or methodology are managed centrally with clear accountability and ownership. Those responsible leverage feedback loops within the syndicate to inform a process of ongoing review.
- Any changes undergo a period of testing to fully understand downstream implications before being implemented for decision making. Subject-matter experts and other teams provide feedback on proposed changes prior to implementation.
- Cyber view of risk and methodology changes are considered as part of a wider syndicate model change framework, with defined triggers and actions to be taken when making updates. Example triggers for review could include major cyber events affecting the market, adoption of new models or approaches, incorporation of loss experience, risk profile changes, inclusion of emerging risks, updates to EJs and so on.

Robustly testing new cyber view of risk methodologies prior to implementation

- Testing of cyber view of risk and methodology changes is managed in line with Sub-Principle 5 ('View of Risk Methodology') and 6 ('View of Risk Validation').
- Methodologies are reviewed and challenged by experts and flow through a defined governance structure.
- Impacts of proposed changes are clearly defined, tested and communicated to decision makers for challenge and agreement prior to adoption.
- Robust testing of any changes to the cyber view of risk and methodologies includes consideration of uncertainty, sensitivity and interdependencies with existing Ejs, which might require resultant updates.
- The internal model can be run ad-hoc when inputs or assumptions are updated or to test wider changes to approach prior to adoption. These changes are considered as part of overall syndicate model change and validation frameworks.

Communicating impacts of cyber changes to decision makers

- Changes should be clearly documented, and downstream impacts on decision making and model outputs well communicated so that any decision makers using the output are aware of a change in methodology and how this might impact their decision making.
- The impact of updating cyber view of risk and methodologies is fed through into decision-making frameworks such as risk appetites and tolerances, and these are updated to reflect changes where appropriate.

Lloyd's principles continued

Sub-Principle 9: Cyber View of Risk Use

Focus on: maintaining consistent understanding, use and continual development of outputs in decision-making processes, i.e. underwriting, portfolio management, strategy, capital setting and risk transfer.

Consistent view of cyber risk used in all downstream decision making

- Cyber exposure analytics, and cyber internal model outputs are integrated with (and support) decision making across underwriting, portfolio optimisation, business planning and strategy and capital setting.
- The cyber view of risk should be consistent across the business, feeding into and supporting all downstream decision making.
- A syndicate's internal model is a working model that can be rerun as and when required. There are triggers set for capital reassessment, which include changes in cyber internal model inputs. Having linked data feeds and degrees of automation allows updates to the current portfolio to be made in a timely way.

Appreciation of cyber limitations and adjustments in decision making

- Training is provided across decision-making teams to ensure there is adequate understanding of cyber internal model input requirements and outputs, including how these should be used and the uncertainties and sensitivities around them.

An effective cyber event response strategy is in place

- Non-natural catastrophe (including cyber) event response plans are documented and include input from exposure management, claims, underwriting, capital, reserving and senior management.
- In the initial stages of an event, a wide range of outcomes and associated uncertainties are considered.
- As an event progresses, feedback loops are in place to inform and adjust current modelling assumptions, cyber view of risk and outputs.
- Suggested improvements are scheduled and tracked.
- Post-event back testing using claims experience contributes to more robust cyber parameterisations.
- Post-event retrospectives are anticipated to consider counterfactuals, i.e. consideration of how much worse the event could have been if the event had breached hours clauses, been malicious instead of accidental, given the time of day the event occurred, response times had been slower/breach had remained undetected, impacted regions and so on.

Incorporation of feedback loops into ongoing cyber view of risk development

- Feedback loops from all cyber view of risk business users are live, clear, tracked and managed. This supports testing of new strategies, impacts of underwriting decisions, reaction to and anticipation of changing market conditions or changes to the cyber view of risk.
- Where outputs do not fit with expectations or current understanding, this is investigated, and a decision is made as to whether an update is required.
- Defined triggers identify where a cyber view of risk review may be required, which may reflect loss ratios or claims data used in benchmarking. Cyber view of risk is included in the areas of the internal model that receive targeted testing as part of scheduled validation work. There is a consideration of materiality in terms of review frequency or other triggers (e.g. change in portfolio mix), which might lead to targeted review/testing. A schedule of development with timed deliverables would be compiled after such a review.
- The internal model can be run as an 'as-if' on an ad-hoc basis to test the impact of view of risk adjustments prior to implementing a decision or strategy.

Lloyd's principles continued

Sub-Principle 10: Governance & Oversight

Focus on: having robust governance and oversight of cyber risk aggregations via a framework that delivers challenge and expertise to ensure the cyber view of risk remains appropriate to continue supporting business decision making.

Robust governance to provide targeted cyber review and challenge

- Exposure management frameworks define a clear cyber-specific governance and decision-making authority structure. This may dovetail with any existing Nat Cat or Non-Nat Cat wider framework, but cyber is discussed explicitly.
- Multiple levels of both technical and strategic review are adopted.
- Adequate understanding of cyber outputs to support decision making
- Those reviewing and using cyber exposure management outputs have sufficient understanding to be able to provide challenge and objective feedback on both quantitative outputs and the approaches adopted to identify, quantify and monitor cyber risk.
- Training, information-sharing and thematic discussions are tailored to the audience, dependent on their decision-making responsibilities and the required depth of understanding. Committees for cyber related decision-making meet at a frequency that is defined by business requirements. There may be regularly scheduled meetings as well as clearly defined triggers for ad hoc meetings, e.g. following an event or when implementing a change in approach.

Ensuring cyber exposure management processes remain appropriate over time

- As approaches to cyber exposure management continue to develop, syndicates similarly develop their oversight and governance frameworks to ensure that they remain adequate.
- Communicate via existing feedback loops between teams and committees, as well as through more formal review.
- Regular cycle and ad-hoc reviews are used to identify where improvements could be made. This can involve the second and third lines of defence and, as required, external third-party input.

Conclusion

Conclusion

"Moving forward, insurers must prioritise robust data governance, continual improvement of modelling techniques and alignment with regulatory frameworks such as the Lloyd's Principles for Doing Business."

The management of cyber risk is a defining challenge of the modern insurance and reinsurance landscape, distinguished by its dynamic, systemic and global nature. As threats grow in scale and complexity, the industry faces a need to evolve its methodologies for assessing and managing these risks. The lack of standardised data schemas, coupled with inconsistent data quality and governance practices, underscores the critical need for a unified approach to exposure management.

Advancements in modelling techniques provide a foundation for improving the industry's capability to manage cyber exposures. Deterministic models, probabilistic approaches and proprietary tools each offer unique strengths in assessing risk, enabling insurers to tailor their methods to align with regulatory expectations and strategic objectives. However, the success of these efforts hinges on the industry's ability to invest in talent, leverage emerging technologies and foster cross-market collaboration.

Moving forward, insurers must prioritise robust data governance, continual improvement of modelling techniques and alignment with regulatory frameworks such as the Lloyd's Principles for Doing Business. By doing so, they can better navigate the complexities of cyber risk, ensuring the resilience and sustainability of the industry in the face of this ever-evolving peril.

lmalloyds.com

Lloyd’s Market Association