Scoping out systemic cyber risk

A framework for assessing the aggregation potential of ‘other cyber’ scenarios

lma
lloyd's market association

Contents

About the LMA

The Lloyd's Market Association (LMA) exists at the very heart of Lloyd's, a world-leading global marketplace for complex risk where solutions to challenges are delivered every day. All 55 Lloyd's managing agencies, with a total market stamp capacity of approximately £52.6bn in 2024, and all Lloyd's members' agents, are members of the LMA.

We represent our members' interests to organisations including governments, regulators, and the market's central supporting body, the Corporation of Lloyd's. We provide professional and technical expertise in areas ranging from model policy wordings to the implementation of innovative technologies. We connect with our members to identify and resolve issues facing the market, and work in partnership with Lloyd's and the other market associations to influence initiatives and outcomes. We operate the market's most comprehensive technical education service, the LMA Academy.

Foreword

The Lloyd’s Market Association (LMA) exists to further the success of our members and of the Lloyd’s market by delivering expertise and education, in addition to connecting and synthesising market opinion. This report is a critical contribution to the ongoing dialogue surrounding systemic cyber risk, providing valuable insights from technical experts in the market to better inform those seeking to navigate this complex and rapidly evolving risk landscape.

In an increasingly interconnected world, where digital networks underpin almost every facet of modern life, the concept of systemic cyber risk has emerged as a critical concern for insurers, policymakers, businesses and individual insureds alike. As our reliance on technology deepens, so too does our vulnerability to the complex and interconnected risks that accompany it. This digital revolution has ushered in a new era of risk, where cyber threats can propagate rapidly across interconnected systems, leading to widespread disruptions and financial losses. Unlike traditional property and casualty insurance risks, which are often confined to individual entities or sectors, systemic cyber risk knows no boundaries, transcending geographical, sectoral and organisational lines.

This report delves into the intricacies of systemic cyber risk, offering a thorough analysis that is both timely and indispensable. By examining case studies and presenting detailed scenarios, the report illustrates the multi-faceted nature of cyber threats and their potential impact on critical infrastructures and industries. It provides a robust framework for understanding and mitigating these risks, emphasising the importance of working with insurers, reinsurers, policymakers and cyber security experts.

One of the standout features of this report is its focus on the aggregation potential of cyber risks – particularly the lesser-known ‘other cyber’ scenarios. The interconnectedness of modern systems means that a single vulnerability can lead to widespread disruptions, underscoring the necessity for advanced risk modelling and comprehensive scenario planning. The detailed examples provided in this report, in the healthcare and maritime sectors, offer valuable insights into how such scenarios can unfold across specific industries with common nodes of aggregation, and the steps required to manage these risks effectively.

Ultimately, effectively managing systemic cyber risk requires a co-ordinated and proactive approach from insurers, policymakers, businesses and other stakeholders. By working together to enhance our understanding of cyber threats, strengthen our resilience to cyber attacks and develop innovative risk management solutions, we can mitigate the potential for catastrophic disruptions.

I commend and thank the authors for their rigorous analysis and thoughtful recommendations, and I trust that their insights will inform and inspire meaningful action across the insurance industry and beyond.

Elizabeth Jenkin
Underwriting Director
Lloyd’s Market Association

1. Executive summary

In the digital age, the rise of cyber security threats and incidents has led to an increased focus on cyber security and cyber insurance.

Within the insurance industry, there is a growing focus on the maturity and completeness of cyber event quantification from company boards, capital providers and regulators.

The most frequently assessed, reviewed and reported systemic cyber events are:

- cloud service provider (CSP) outage
- widespread ransomware
- mass data breach
- critical infrastructure blackout.

While cyber modelling remains, relatively speaking, in its adolescence, the potential insured impact of these systemic events has been reviewed frequently by risk modelling vendors, Lloyd's, regulators and internally within many insurance companies.

However, given the increase in digitalisation of almost every industry, there is an ever-growing number of 'other cyber' scenarios that could occur. While these scenarios may not reach the severity of the four most common events outlined above, they can still result in material losses in specific industries with common nodes of aggregation, with any insured losses likely to be focused outside or in addition to the standalone cyber market.

This report seeks to provide insights for executives, underwriters of all classes and claims managers into the potential of other cyber exposures associated with increasing digitalisation in the industry.

It further provides a practical framework for exposure management practitioners and risk managers for reviewing relevant information, identifying critical industry systems and critical nodes of aggregation, and for developing quantifiable deterministic scenarios.

1.1 Purpose

The purpose of this report is to propose a framework for identifying, understanding and quantifying potential 'other cyber' scenarios.

Two example systems have been used to illustrate the application of the framework. These systems are critical for their respective industries, and their disruption could lead to significant insured losses. Managing agents and insurers should undertake their own research and analyse how these or other nodes of aggregation may impact their portfolios.

- **Healthcare**
  An Electronic Health Record System (EHRS) stores the patient's electronic medical record, including specific private information relevant to that person.
- **Maritime shipping**
  An Electronic Chart Display and Information System (ECDIS) is an electronic geographical nautical navigation system onboard vessels.

These examples use a bottom-up approach to calculate losses. However, a lack of detailed information should not be a barrier to expanding loss scenario suites; therefore, it may be necessary to use a top-down industry loss approach by class for certain coverages or non-standalone cyber classes.

1. Executive summary continued

1.2 Rationale

Evolving cyber risk and regulatory landscape

The rise of internet use and the increase in digitalisation has led to cyber attacks becoming more sophisticated and profit-oriented.

Frequency trend analyses show that since before the COVID-19 pandemic, the number of cyber attacks has almost doubled (Figure 2) with malicious data breach and ransomware incidents being the main drivers of economic and insured loss.

Regulation

Against this increasing threat, insurance companies are required to monitor their accumulation of cyber exposures, which can lead to potential claims arising from either cyber-specific policies or from policies whose primary cover is not cyber risk, such as directors’ and officers’, general liability, healthcare, marine and others.

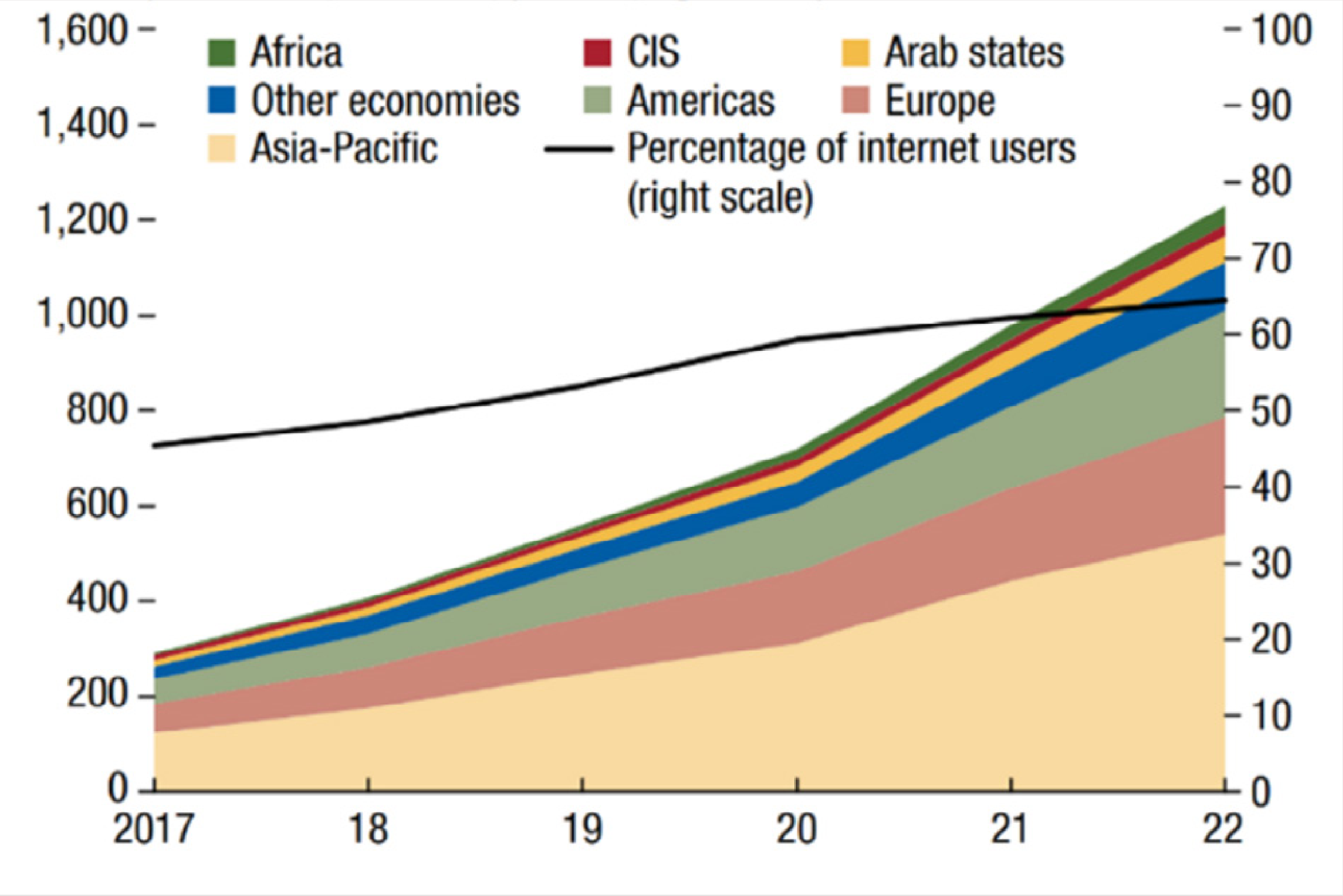
Modelling approaches

To model and quantify cyber risk, new approaches have been developed and existing ones continue to be enhanced, led by (re)insurers, brokers, risk modelling vendors, regulators and academics. Despite the progress made thus far, cyber models remain immature, especially compared to those developed for natural catastrophe perils, and their outputs can change significantly year-on-year.

As an auxiliary tool, insurers can develop deterministic scenarios to assist with assessing cyber risk in their portfolio. These scenarios can be adjusted relatively easily to identify potential cyber losses within specific classes, products and/or industries where each (re)insurer has a high concentration of exposures.

Figure 1

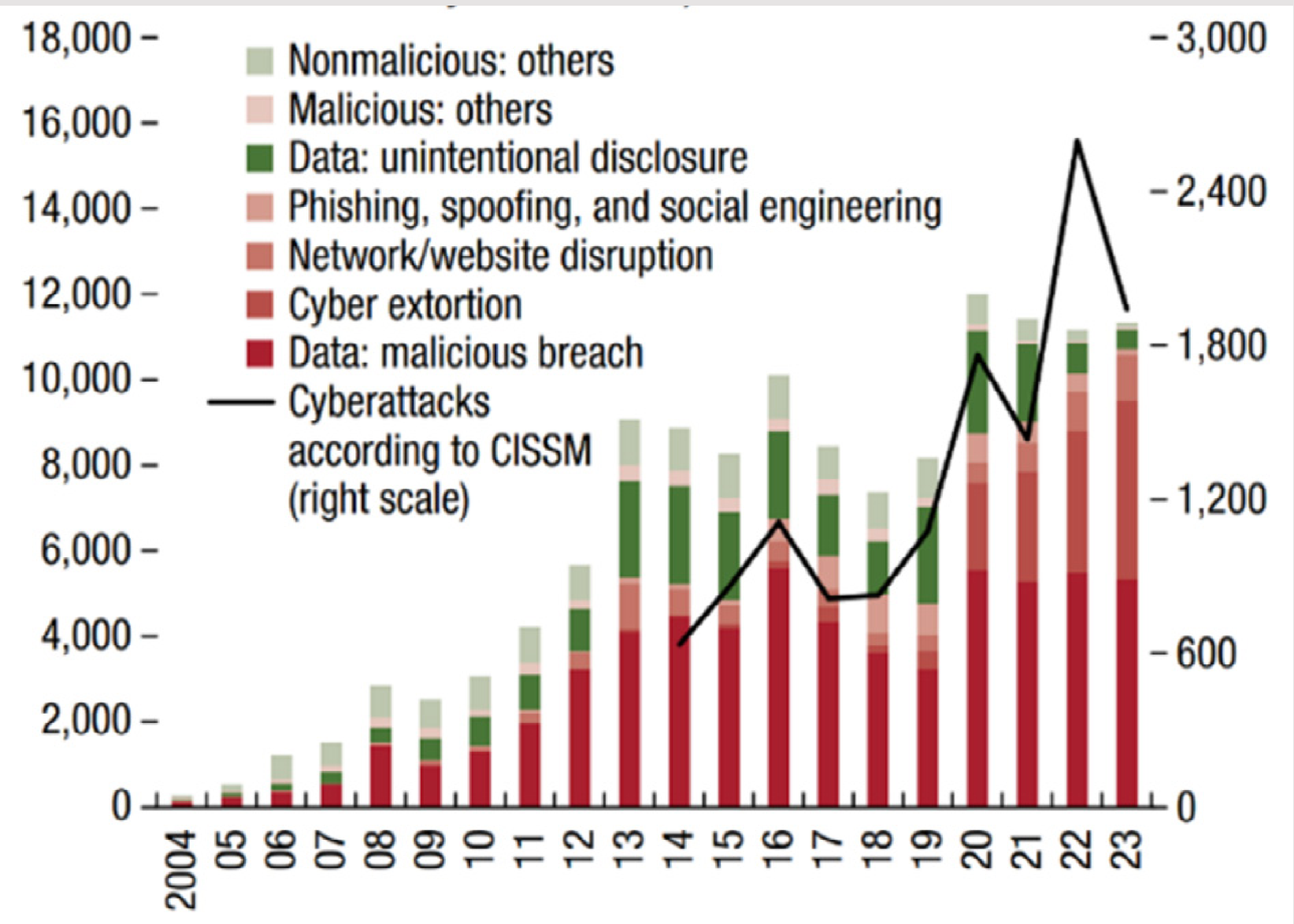
Internet use and international bandwidth use
(Trillion bits, leftscale; percent, right scale)



Source: International Monetary Fund, Global Financial Stability Report, April 2024.

Figure 2

Global number of cyber incidents 2004-23



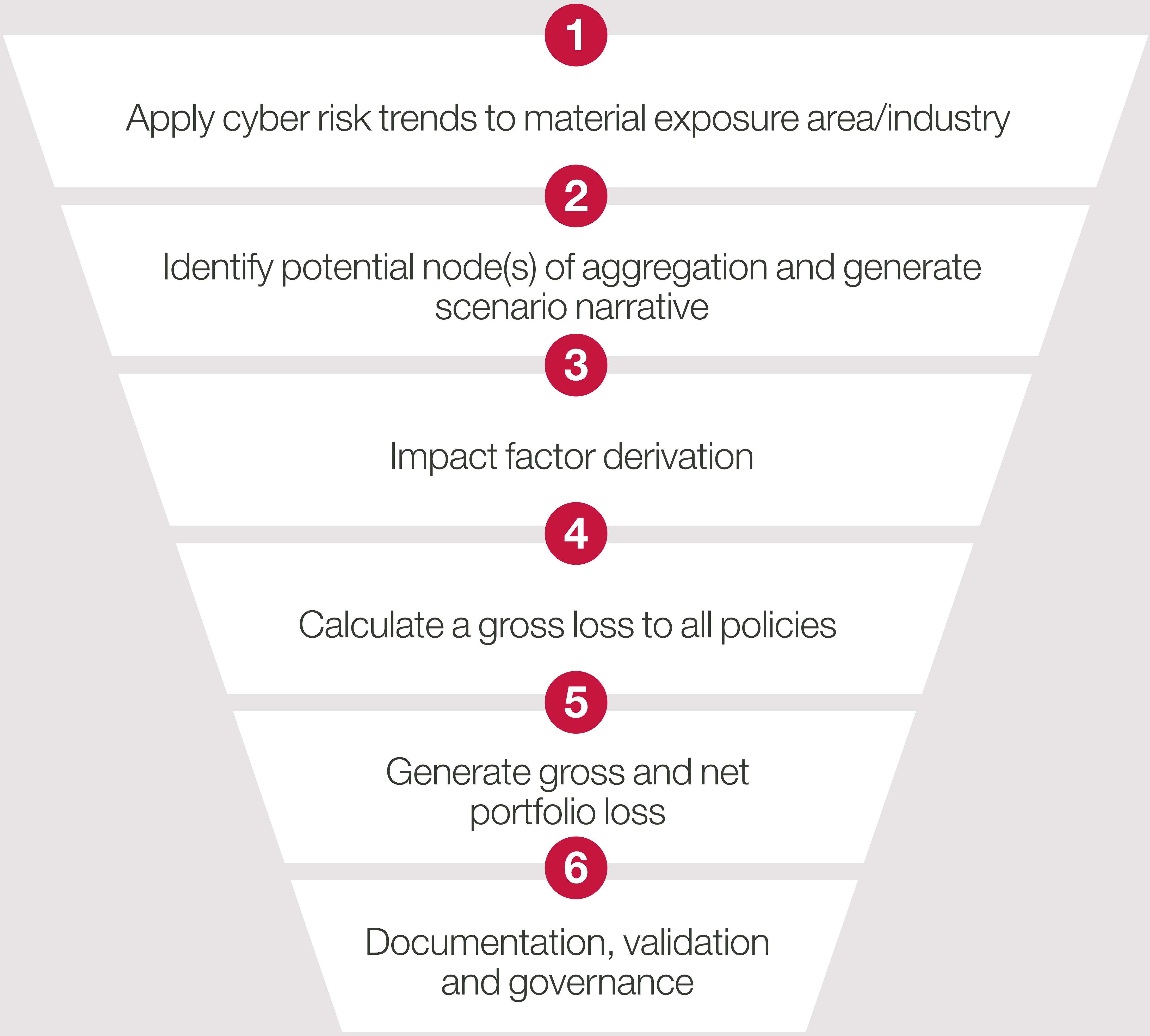
Source: International Monetary Fund, Global Financial Stability Report, April 2024. The right-hand scale shows data on cyber attacks from the Center for International and Security Studies at Maryland (CISSM).

2. The framework

The step-by-step process proposed below provides a structured framework to support practitioners in identifying, understanding and quantifying potential 'other cyber' scenarios.

The following sections provide more detail for each step of the framework. This is then applied to the two examples.

Figure 3
Cyber risk framework


1
Apply cyber risk trends to material exposure area/industry
2
Identify potential node(s) of aggregation and generate scenario narrative
3
Impact factor derivation
4
Calculate a gross loss to all policies
5
Generate gross and net portfolio loss
6
Documentation, validation and governance

2.1 Apply cyber risk trends to material exposure area/industry

In preparation for generating a scenario, there should be an assessment of the latest cyber risk trends that could impact the exposure area/industry of interest. These could include broader trends seen elsewhere that could then impact the selected area/industry, or they could be industry-specific trends.

Recent cyber events, even in unrelated industries, could help identify possible nodes of aggregation that could be vulnerable to future cyber events. The table of cases (section 4) provides some examples that could be utilised in the first instance.

2.2 Identify potential node(s) of aggregation and generate scenario narrative

Increased digitalisation within almost every industry means that an increase in 'technology risk' is adding to or increasing the potential aggregate losses across multiple insureds through new or existing nodes of aggregation. These nodes of aggregation could include commonly used software or critical equipment or systems providers that could be vulnerable to a cyber event, as a result of either non-malicious or malicious events, with the potential aggregation in terms of the number of users being the same in both cases.

Understanding critical systems by industries and the consequences of their disruption may be supported by additional expertise to identify, prioritise and, importantly, to understand the impact of system failure. This may include industry experts not limited to cyber.

2. The framework continued

The initial focus of a new scenario should be on the aggregation potential rather than the specific causes of the event, as there may be multiple routes to the same critical system failure, both malicious and non-malicious. However, the ability to specify the nature, scope, likelihood, severity and loss development (over a period of time) within the scenario can help determine the insurance policies in scope that could generate losses.

Assumptions may later require stress testing or may lead to scenario variations. However, reviewing industry trends or conducting scenario analysis could be used to simulate potential outcomes of the event under different circumstances and severity levels (for example, flexing factors such as event intensity, duration and affected industries), and assist with identifying alternative scenarios that could follow the steps of this framework.

2.3 Impact factor derivation

Once the scenario has identified the potential aggregation of a critical system, an assumption is needed for what proportion of companies are likely to be impacted and will suffer a loss. Further consideration needs to be given to:

- The proportion of companies that use or are exposed to the identified critical system.
- Of those companies exposed, the likely proportion that will be impacted/exploited.

Data may be available to support the parameterisation of insureds exposed, for example, by reviewing market share of a selected critical system. This information may be accessed by conducting market research, licensing external datasets and/or consulting with internal and external experts. The proportion of insureds impacted/exploited is likely to be more of a subjective assumption and heavily reliant on expert judgement.

The scenario should be constructed carefully to help inform this. Factors for consideration may include:

- A vulnerability assessment to identify weaknesses in the critical system that could be exploited.
- Analysis of the current threat landscape and the likelihood of cyber attacks targeting the critical system or industry.
- Availability of patching for non-zero-day vulnerabilities, and the patching adoption rate and delay, by industry or company size.
- Whether the failure is due to error or exploitation.
- Sophistication of potential threat actors and scale of any attack, such as single or multiple threat actors and their global outreach:
  - A 'Kill Chain' analysis could be conducted to assess how easily this particular scenario vulnerability can be exploited and achieved at scale.
  - There may be an upper limit on the data storage and exploitation capability of the threat actor.
  - The key motivator of the threat actor – whether disruption, financial gain or data theft.
  - The threat actor's level of resources.
- The function of the critical system, including its role in supporting key business operations or data management and whether alternatives or backups are likely to exist.
- Accessibility of the system, such as network connectivity (internal or external), third-party dependencies and potential entry points for attackers.
- Whether the likely proportion impacted varies between companies with smaller and larger revenues.
- The safety and security measures, incident response capabilities and resilience of the impacted industry or portfolio.

The final proportion of companies suffering a loss – the impact factor – would be calculated by multiplying the proportion of companies vulnerable to the critical system by the proportion of vulnerable companies assumed to be exploited/impacted.

2. The **framework** continued

2.4 Calculate a gross loss to all policies

Once a node of aggregation has been identified and the impact of the critical system is understood, the total insured exposure to the scenario can be considered.

Assuming at this stage that all insureds within the identified industry are impacted, consideration needs to be given to all potential coverages affected and types of losses the scenario could cause, including but not limited to:

Standalone cyber coverages	Non-standalone cyber classes/coverages
Business interruption	**Classes**
Incident costs (customer notification costs, call centre costs, crisis management, forensics/IT, public relations)	Property and casualty (P&C)
	Professional indemnity (PI)/errors and omissions (E&O)
Data restoration or recovery	Medical malpractice
Regulatory defence costs	Directors' and officers' (D&O)
Third-party coverage	**And classes with coverage, including:**
Settlement payments (liability costs), e.g. to hospitals and patients	Physical damage – property/marine
	Business interruption/loss of hire
Legal defence costs	Third-party liabilities
Network security liability	Bodily injury
Fines and penalties	Financial losses (including pure financial loss)

The ground-up loss severity needs to be parameterised for all policies by consolidating the component parts, such as revenue generation impacts, regulatory fines, notification and monitoring costs, and third-party liability. This should include the impact of regional and jurisdictional differences.

This could involve analysing historical data and past occurrences of similar events, including those that may have occurred due to non-cyber triggers historically.

When using past claims data, consideration should be given to the possible differences in costs between a large-scale accumulation event and an event impacting a single insured company. For example, economies of scale for forensic review or the lack of appropriate resources leading to price surges should be taken into account.

Policy terms are then applied to the ground-up loss to derive a gross loss for each policy, which allows for sub-limits, deductibles and exclusions.

2.5 Generate gross and net portfolio loss

Once the impact factor has been determined and the gross loss severity for all policies has been constructed, various methods exist for selecting which insureds will be impacted, including:

- Assume that each insured is equally likely to be impacted and therefore multiply the calculated gross loss for each policy by the impact factor and sum across the entire portfolio.
- Assume that some insureds are more or less likely to be impacted and therefore assign a weighting to each policy as part of the calculation above.
- Use stochastic modelling to generate multiple simulations. In each simulation, a random subset of insureds is assumed to be impacted, with the overall proportion in line with the impact factor. Consider the mean and range of potential outcomes to understand the sensitivity of the portfolio to the distribution of losses.

Ideally, all losses are considered on a ground-up, policy-by-policy basis. However, at this stage, any final consideration for losses where detailed information is not available and not previously captured in the loss calculation should be made.

A top-down approach can be utilised including, but not limited to, market share data, proxy portfolios, expert judgement, or historical losses – with adjustments as needed.

Reinsurance programmes should be applied as per their policy terms and conditions and any recovery should consider existing erosion of limits. Particular care should be given to the review of cyber exclusions and reinsurance cyber aggregation exclusions when considering whether back-to-back cover is in place.

2. The framework continued

Different covers can be applied as follows:

- Proportional reinsurance can be applied to the policy losses by year of account, with consideration given to any aggregate caps.
- Event XL, aggregate excess of loss, stop-loss and CAT bond covers can be considered using the total gross or net of proportional reinsurance losses, as appropriate, from the earlier calculation steps.
- For per risk excess of loss covers, assumptions may need to be made regarding the number of risks impacted if the gross loss is determined by applying the impact factor to all policies weighted equally.

2.6 Documentation, validation and governance

Documentation and validation of the scenario narrative and loss calculations should be carried out in line with Solvency II standards. Validation activities could include:

- Strengths and weaknesses of selected methodology and consideration of alternatives.
- Sensitivity testing on key parameters.
- Peer review of methodology and loss calculations.
- Independent review by individuals not involved in the design and build, by internal working groups/committees, and/or through third-party/external expert review if appropriate.
- Risk ranking (loss comparison) against an existing scenario suite.
- Back-testing against any relevant historical losses.

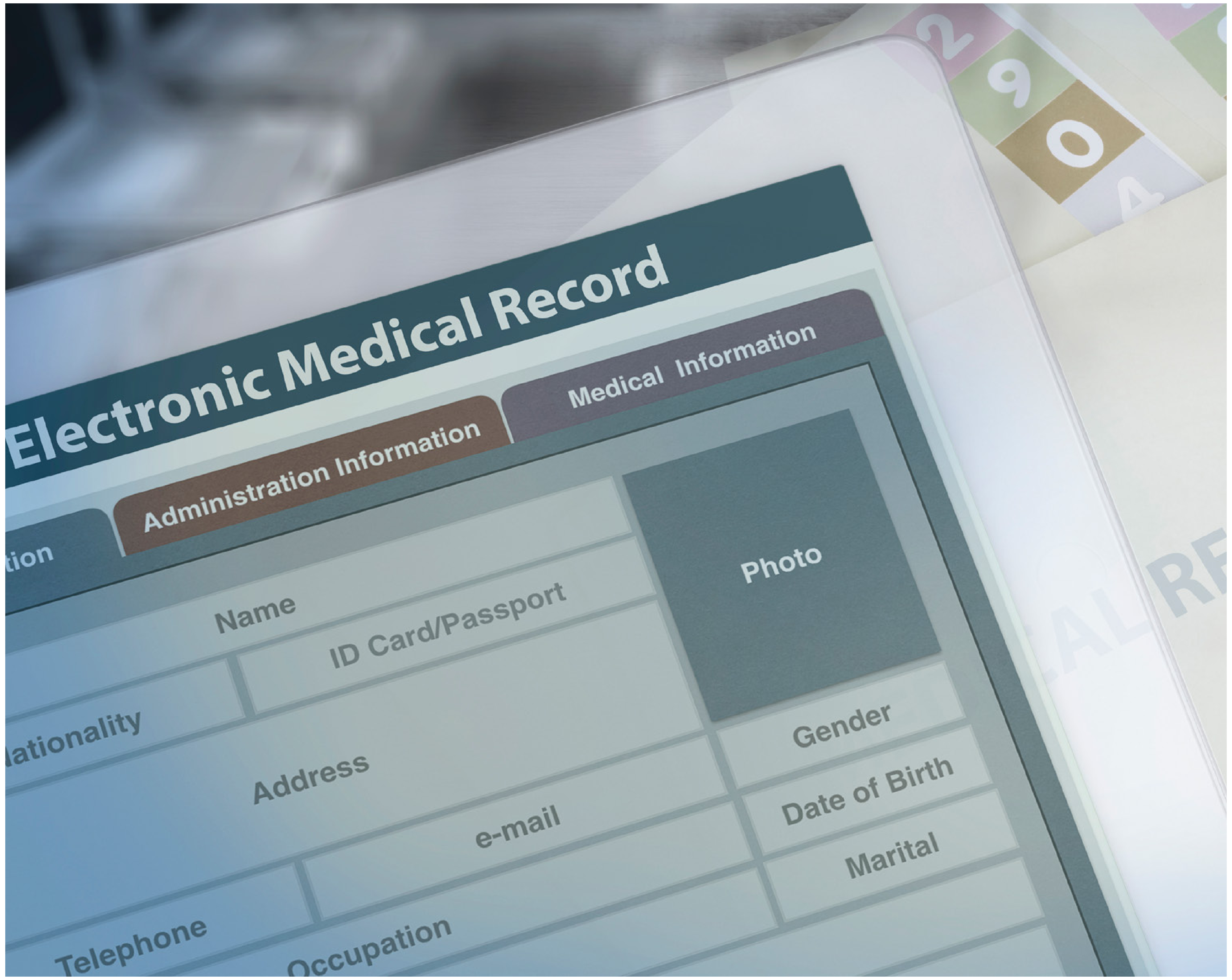
Validation of key assumptions and expert judgement should be an ongoing process as the scenarios are developed, or as additional information becomes available.

Governance processes need to be in line with existing scenario development, including the cadence of review. Several factors will be influenced by external events and change over time, and therefore these scenarios should not be static.

3. Framework examples

Example scenarios have been built out for the healthcare and maritime industries to illustrate the process defined above. While these scenarios may be more relevant to some carriers than others, all carriers will have some lines of business or insured industries with aggregate digital technology risks, for which a similar process can be followed. The detailed framework example for these industries can be found in the sections that follow.

3.1 Healthcare example



The goal of this example is to provide an approach for parameterising a systemic scenario within the context of an attack on an Electronic Health Record System (EHRS).

i. Apply cyber risk trends to material exposure area/industry

The insurer has assessed their portfolio and concluded that it is exposed to the healthcare industry. It has been identified as an industry with cyber aggregation potential, therefore warranting the creation of a scenario to measure and quantify the risk.

A recent example of this is the Change Healthcare cyber attack on 21 February 2024, which highlighted the potential systemic impact arising from a common vulnerability in the healthcare industry – this worked example is not based on that event.

The healthcare industry has a significant quantity of valuable data, including patient records, which is required to carry out procedures and prescribe medication.

ii. Identify potential node(s) of aggregation and generate scenario narrative

The insurer, having identified the healthcare industry as an aggregation risk, begins the process of building a scenario narrative. This will involve research into critical healthcare technologies which could be exposed to a malicious or non-malicious event resulting in an insured loss. This may require consultation with experts in the field, whether internal or external to the insurer.

Research indicates that patient records are now computerised and interconnected systems, such as EHRS or Electronic Medical Record Systems, are often used in hospitals. These are either cloud-based, storing data on external servers and accessible by any device that has an internet connection, or server-based, storing data on either a personal server or in a data centre.

Such systems allow the electronic entry, storage and maintenance of digital medical data or contain the patient's records from doctors and include demographics, test results, medical history, history of present illness (HPI) and medications.

3.1 Healthcare **example** continued

The insurer identifies EHRS as a critical node of aggregation which could lead to an insured loss if disrupted. The insurer constructs the following scenario narrative, whereby a widely used on-premise EHRS is disrupted.

For the purposes of this example, the EHRS provider directly impacted will be referred to as 'Healthy Records':

A zero-day vulnerability in the Healthy Records system is exploited by a single threat actor to gain unauthorised access. Healthy Records is an internet-facing on-premise EHRS. The attack impacts multiple customers of Healthy Records. The threat actor is able to compromise sensitive medical data, impacting the confidentiality, availability and integrity of the data. First and third-party liability claims follow, in addition to regulatory fines.

iii. Impact factor derivation

The scenario has identified the potential aggregation of a critical system provided by Healthy Records.

The scenario narrative in step ii) states that only those using the Healthy Records EHRS are exposed to the event, and that only a subset of these are actually exploited by the threat actor.

Therefore, an assumption is needed for what proportion of healthcare policies cover risks using Healthy Records, and within this subset, the proportion that are exploited and suffer a loss:

- What proportion are using Healthy Records?
  The insurer conducts research which suggests Healthy Records has a market share of 37% and rounds up to 40% for prudence.
- Of those using Healthy Records, which of those exposed to the vulnerability are then exploited?

The scenario narrative describes this vulnerability as a zero-day, so the insurer assumes all users of Healthy Records have the vulnerability, so there is no discount for patching.

The scenario narrative describes this event as happening at scale, i.e. more than one healthcare provider is impacted. However, as the attack is not automated, and there is a single threat actor (scenario detail), there will be an upper limit to how widespread the event can be.

This assumption is driven by both internal and external expert judgement. In this example, the insurer has considered a 'Kill Chain' analysis, i.e. how easy this particular scenario vulnerability is to exploit and achieve at scale. Data theft is assumed to be the key motivation for the threat actor, therefore, there is an upper limit on the data storage and exploitation capability of the single threat actor.

Based on the above, the final assumption used is that 20% of those using Healthy Records are attacked and suffer a loss.

Therefore, the final proportion of insureds suffering a loss can be calculated as:

$$Prop_{loss} = Prop_{healthy\ records} \times Prop_{vuln} \times Prop_{exploited}$$

$$Prop_{loss} = 40\% \times 100\% \times 20\% = 8\%$$

For example, assuming 500 policies within the healthcare industry in the insurer's portfolio, and the above 8% example assumption, the insurer would have 40 individual policies generating losses within this scenario.

This is a highly uncertain and subjective assumption, which must be supported by internal and external expert judgement, and with thorough review and oversight.

3.1 Healthcare **example** continued

iv. Calculate a gross loss to all policies

Given that the scenario impacts the healthcare industry, the insurer collects all its exposures (including policy data and firmographic data where available) for all policies within the healthcare industry across product lines.

The insurer then considers:

What classes of business are impacted by this scenario?

- Cyber.
- Medical malpractice as a result of data integrity failures, treatment refusal or delay.
- Directors’ and officers’ liability.
- Professional liability for breach of privacy, fines and penalties, where insurable, for impacted firms without a cyber policy or inadequate limits.

What type of data is accessed?

- Protected Health Information (PHI) – Data regarding a patient’s health record, protected by regional data protection acts, for example, the US Health Insurance Portability and Accountability Act (HIPAA) 1996.
- Personally Identifiable Information (PII) – Data which can be used to identify an individual directly or indirectly. Protected by various regional privacy acts, such as the Privacy Act of 1974 in the US and the General Data Protection Regulation in the EU.
- Payment Card Industry data (PCI) – Data containing payment and credit information of customers, or patients in this case.

What coverages does this scenario impact?

- Forensics and incident response costs.
- Direct and/or contingent business interruption.
- Notification and monitoring costs.
- Regulatory fines.
- Third-party liability costs.
- Legal defence and settlement costs.

With this information, the insurer begins the process of parameterising the ground-up loss per insured. Where expert judgement has been used, the insurer records the rationale and governance that supports its use:

- Regulatory fines, for example, for breaching HIPAA data protection rules:
  - The insurer uses a mixture of expert judgement and data on fines from past events. The insurer expresses the fine as a percentage of each insured’s revenue.
- Forensics and incident response costs:
  - Historical claims data from past data breaches is used by the insurer to derive an assumption by revenue size. Where claims data is missing or sparse, the insurer uses internal expert judgement.
- Notification costs:
  - Notification and monitoring costs scale with the number of records impacted in the breach. Therefore, an assumption around record counts (using expert judgement in the absence of any other data source) is made by the insurer. This assumption varies by revenue size of the insured.
  - Existing agreements with third parties for monitoring and notification costs following a breach are used by the insurer. Historical claims data could also be used. These costs are typically stated per record and per record type, for example, PHI, PII and PCI.
- Third-party liability claims:
  - Individuals impacted by the data breach may become involved in class actions against the insured. This could result in both a legal settlement cost and a legal defence cost. Batch legal claims, such as class actions, would expose the insurer and minimise the impact of any ‘each and every loss’ retention on the policy.
  - The insurer generates an assumption for these third-party liability costs per insured by reviewing historical data and/or using internal expert judgement.
  - These assumptions may vary by revenue of the insured. The scale of the event may also influence the size of any third-party losses. This may be seen most in D&O claims and in non-zero-day events. In these cases, blame can be more fairly assigned to the insured if they did not take action to minimise the risk, for

3.1 Healthcare example continued

example, by patching known vulnerabilities or performing appropriate security risk assessments.

With all the assumptions determined above, the insurer can now calculate a total gross loss per policy by applying the relevant policy terms. Note, policies will often include various sub-limits, deductibles and exclusions which should also be factored into the gross loss calculation for each insured. For simplicity, there are no sub-limits or relevant terms and conditions in this example.

v. Generate gross and net portfolio loss

The insurer has so far assumed that every policy within the healthcare industry is generating a gross loss from step iv). The insurer has made no decision as to which policies are impacted by the event. The insurer then assumes that each policy is equally likely to be impacted, and so multiplies the calculated gross loss per policy, by the proportion suffering a loss from step iii), and sums across the whole portfolio:

$$Portfolio\ Gross\ Loss = \sum_{i=1}^{n} Policy\ Gross\ Loss_i \ \times Prop_{loss}$$

$$n = total\ policies$$

If the insurer had decided that some policies are more or less likely to be impacted, a weighting could have been assigned to each policy as part of the calculation:

$$Portfolio\ Gross\ Loss = \sum_{i=1}^{n} Policy\ Gross\ Loss_i \ \times Policy\ Weighting_i \ \times\ Prop_{loss}$$

$$n = total\ policies$$

For example, a larger revenue risk might appear a more valuable target for the threat actor and therefore more likely to be attacked than a smaller revenue risk. This could also be approached by the insurer calculating an assumption for multiple revenue sizes.

To generate a net loss, the insurer should then consider applicable reinsurance arrangements that are in place and apply these terms to the gross losses. This may be applied in aggregate (for example, aggregate excess of loss or quota share) or on a risk-by-risk basis (for example, variable quota share or risk excess of loss).

3.1 Healthcare example continued

vi. Documentation, validation and governance

The insurer applies the general steps set out in the framework above. The following lays out some additional considerations the insurer could have explored as part of their validation:

- The insurer has considered only an on-premises EHRS. Varying the narrative to a cloud-based EHRS may change the scenario loss, and lead to different management decisions.
- The insurer has assumed that the insured is using only one EHRS. How would the loss vary if they used multiple EHRS providers?
- In certain regions, use of EHRS might be less widespread. Should the insurer consider whether all the insureds are using an EHRS in the first place before applying the market share for a given provider?
- The insurer has considered a malicious scenario. How would the loss vary if this scenario was non-malicious?

3.2 Marine example

The goal of this example is to provide an approach for parameterising a systemic scenario within the context of a critical operational technology system/industrial control system that results in loss of use and physical damage. This example utilises an attack on an Electronic Chart Display and Information System (ECDIS) specific to maritime. This approach can be applied to a multitude of industries and operational technology.

Intentionally, the event description is malicious/intent to do harm, for which there is exclusionary language in most instances. When applying this or other developed scenarios, the insurer may want to consider the potential for a technological ‘node of aggregation’ to be impacted as a result of an error or third-party provider error. The CrowdStrike-Microsoft defender outage was an example of a service provider error resulting in the loss of systems.

Insurers should also consider cover provided via buybacks to exclusions and/or participations on reinsurance treaties.

i. Apply cyber risk trends to material exposure area/industry

The insurer has assessed their portfolio and concluded that it is exposed to the maritime industry generally, which has been identified as having cyber aggregation potential. Therefore, it warrants the creation of a scenario to measure and quantify the risk.

The maritime industry is increasingly digitised, with interconnected systems onboard, connected to shoreside operations. This is contributing to an increasingly complex supply chain and a larger potential attack surface.

There are attack surfaces and potential vulnerabilities across critical operating systems that utilise information and operational technology for navigation, ships’ ballast, cargo management systems and propulsion.

These risks have been increasingly recognised in recent years, most recently with the extension of the United States Coast Guard’s powers, new cyber design requirements for newly built vessels and an expected fourth update of the International Maritime Organization’s (a United Nations agency) Guidelines on Maritime Cyber Risk Management.

ii. Identify potential node(s) of aggregation and generate scenario narrative

The insurer, having identified the maritime industry as an aggregation risk, begins the process of building a scenario narrative. The US Coast Guard’s 2023 cyber trends report identifies three potential systems that could be exploited or are vulnerable to human error.

These systems are:

- Integrated navigation systems, for example, Electronic Chart Display and Information System (ECDIS)
- Cargo management systems
- Automatic Identification Systems (AIS)

3.2 Marine **example** continued

Of the three scenarios, the insurer identifies ECDIS as having the most potential as a systemic node of aggregation, with regulations requiring it to be frequently updated and using third-party suppliers/vendor software.

The US Coast Guard report is a useful source document which is freely available. It is not vessel-specific or exhaustive and there are additional critical systems on vessels.

A cyber security incident affecting ECDIS could be triggered by a spear phishing attack, a corrupted update, through USB key ports, or through the use of old equipment and operating systems which have not been updated.

The insurer constructs the following scenario narrative, whereby a widely used ECDIS service provider is compromised. For the purposes of this example, the ECDIS directly impacted will be referred to as 'Nav Charts':

A threat actor, seeking financial gain, launched a targeted malware attack on the largest ECDIS by market share, Nav Charts, following a successful spear phishing campaign. Malicious code is embedded in the weekly chart firmware update received by all their clients; it is then activated one week later, leading to a loss of navigation systems and further failures in interconnected systems.

The impact of this cyber attack is mitigated pre-and post-event by a number of existing marine practices, including the use of sandboxing of updates before releasing them to the ship, manual backup protocols and manual navigation. A vessel's proximity to port, and the assistance from vessel control authorities, nearby vessels and onboard engineers would reduce the number of vessels sustaining physical damage.

A residual number of vessels are rendered inoperable until external service engineers can gain access. Passage is suspended and some vessels remain in port due to statutory deficiency.

iii. Impact factor derivation

The scenario has identified the potential aggregation of a critical system, ECDIS; assumptions are now needed for what proportion of companies are impacted and will suffer a loss.

With a combination of external expert input and desk-based research, the following items are identified:

- **ECDIS vendors:** The world-leading provider has over 35% of the ECDIS world market share and a dominant Number 1 position in ECDIS. To be prudent we have used a market share of 37%.
- **ECDIS update:** The majority of the world's fleet is now fitted with ECDIS. A proportion of vessels with ECDIS will apply updates pre discovery. Therefore, it is assumed the highest possible proportion of vessels (88%) that can install the update within one week will do so.
- **ECDIS reliance:** Some vessels may be provided with a backup ECDIS or set of paper charts for certain scenarios. A conservative assumption is made that 90% rely on an ECDIS provider or don't have paper charts.

The assumptions above allow the insurer to determine the proportion (PropExpos) of vessels on the insurer's book that are utilising NAV Charts and exposed.

Therefore, the final proportion of insureds open to suffering a loss can be calculated as:

$$Prop_{Expos} = Prop_{NAV\ Charts} \times Prob_{Adop} \times Prob_{rel}$$

$$Prop_{Expos} = 37\% \times 88\% \times 90\% = 29\%$$

3.2 Marine **example** continued

The insurer then needs to identify what the resultant loss could be to the proportion of their fleet with ECDIS malware issues. This is done with a combination of external expert input and desk-based research. The following items are identified as potential areas of loss; the extent of policy application is considered in the next section:

- The number of vessels in port or at anchor at time of ECDIS failure – 13% based on UNCTAD data review.
- 7% of vessels identified as operating in busy shipping lanes/passage (confined waters/vulnerable positions) at any one time.
- Vessels in vulnerable positions would likely require an element of human error following the loss of ECDIS in order to incur a marine casualty event and physical damage. This can be considered using claims expert opinion and/or claims data causality. For this example, 10% human error has been used.
- Vessels in open water have negligible risk of physical damage as a result of ECDIS outage.
- The maximum period of time to get to port under normal navigation practices is 22 days.
- For simplicity of this example we have assumed that 50% of vessels return and are restored within 14 days, and 50% take the maximum 22 days and that vessels are fully restored within five days of return. Other return and restoration patterns could be considered.
- Wait period deductibles typically apply to coverages linked with delays. These can range from 3 to 21 days. In this example, 14 days has been used as a reference point. The extent of coverage is considered in the next section.
- For vessels that suffer physical damage, hull claims can be used as a proxy for damage factors.

ECDIS down = 29.3%
37% x 88% x 90% = 29.3%

Loss of vessel use

Physical damage/ loss of vessel use

At port with ECDIS down
29.3% x 13% = 3.8%

At sea with ECDIS down but not in busy lane
29.3% x 87% x (100%-7%) = 23.7%

In busy lane with ECDIS down
29.3% x 87% x 7% = 1.8%

ECDIS restored in 14 days waiting period: no loss of hire

50% return and restored within 14 days: no loss of hire

50% return and restored within 27 days (23.7% x 50% = 11.9% loss of hire impact factor)

No human error: 90% return and restored within 14 days: no loss of hire or physical damage

Human error: 10% suffer physical damage loss (1.8% x 10% = 0.2% physical damage impact factor)

3.2 Marine **example** continued

iv. Calculate a gross loss to all policies

Given the scenario impacts the maritime industry, the insurer collects all its exposures (including policy data and firmographic data where available) for all policies within the maritime industry across product lines.

The insurer then considers:

What classes of business are potentially impacted by the scenario generated?

- Hull and machinery
- Loss of hire
- Marine war
- Cargo
- Cyber (risk codes CY and CZ)
- D&O

With this information, the insurer begins the process of parameterising the ground-up loss per insured. Where expert judgement has been used, the insurer records the rationale and governance that supports its use:

- Hull and machinery – physical damage has been accounted for in the impact factor analysis; there should be consideration of additional costs associated with sue and labour, recover to port, etc. Physical damage, where there is intent to do harm via cyber means, is typically excluded under hull and machinery policies. However, several buyback facilities and reinsurance treaties are supported by the market and should be reviewed for inclusion.
- Hull and machinery regulatory fines, such as Port Authorities and/or Flag state.
  - The insurer uses a mixture of expert judgement and data on fines from past events. The insurer expresses the fine as a percentage of each insured's revenue.
- Marine war – malicious cyber cover may be given in a marine war policy and may not require physical damage, depending on the individual wording.
- Cargo – standard policies likely require a physical damage trigger and delay is often excluded. There may be spoilage cost associated with delayed vessels and any loss of cargo associated with the physical damage. The insurer uses a mixture of expert judgement on the proportion of cargo ships and the volume of perishables within the cargo account and level of coverage given.
- Loss of hire – has been accounted for in the impact factor analysis. However, 'physical damage' in relation to damage to the ECDIS is dependent on the definition of physical damage and/or the potential for 'non-physical damage' cover under P&I club buybacks, etc. There should be consideration of additional costs or third-party impacts. For example, if an insured is not directly impacted by the cyber event, would there be coverage under berth blockage, etc. if their journeys are disrupted?
- Cyber CZ – affirmative cover for the physical damage offered by the cyber market, both directly and via facilities and consortiums, should be accounted for. This could be under a marine cyber buyback, affirmative reinsurance of P&I club buyback language or cyber policies with physical damage add-ons.
- Cyber CY – business interruption. The definition of computer systems should be considered as it applies to insureds' onboard systems. Dependent/contingent business interruption for insureds that may be reliant on goods being transported is also in scope. And in addition, for the impacted service provider, there is the consideration of extortion payments and forensics and incident response costs.
  - Historical claims data from past data breaches is used by the insurer to derive an assumption by revenue size. Where claims data is missing or sparse, the insurer uses internal expert judgement.
- Legal defence and settlement costs.

With all the assumptions determined above, the insurer can now calculate a total ground-up loss per policy by applying the relevant policy terms. Note, policies will often include various sub-limits, deductibles and exclusions which should be factored into the gross loss calculation for each insured. This example application of the framework sets out a possible event rather than any confirmation of policy cover or application of exclusions. For simplicity, there are no sub-limits or relevant terms and conditions in this example.

3.2 Marine example continued

v. Generate gross and net portfolio loss

The insurer has so far assumed that every policy within the hull and machinery and loss of hire portfolio is generating a gross loss from step iv. The insurer has made no decision as to which policies are impacted by the event.

The insurer then assumes that each policy is equally likely to be attacked, and so multiplies the calculated gross loss per policy by the proportion suffering a loss from step iii, and sums across the whole portfolio for both the loss of hire impact factor and physical damage impact factors:

$$Portfolio\ Gross\ Loss = \sum_{i=1}^{n} Policy\ Gross\ Loss_i \times Prop_{Expos}$$

$$n = total\ policies$$

If the insurer had decided that some policies are more or less likely to be attacked, a weighting could have been assigned to each policy as part of the calculation:

$$Portfolio\ Gross\ Loss = \sum_{i=1}^{n} Policy\ Gross\ Loss_i \times Policy\ Weighting_i \times Prop_{Expos}$$

$$n = total\ policies$$

Other impacted classes can be applied using average line sizes for the proportion of an impacted insured, based on expert judgement.

In consideration of other lines of business, for example, cargo and cyber in step iii, the insurer uses portfolio information, average line size and claims history, and size of loss to inform the calculations and to include these classes into the overall losses.

To generate a net loss, the insurer should then consider applicable reinsurance arrangements that are in place and apply these terms to the gross losses.

This may be applied in aggregate (e.g. aggregate excess of loss or quota share) or on a risk-by-risk basis (e.g. variable quota share or risk excess of loss).

vi. Documentation, validation and governance

The insurer applies the general steps set out in the framework (2.6). The following lays out some additional considerations the insurer could have explored as part of their validation:

- The insurer considers the potential for the technological node of aggregations to impact vessels in a similar way.

  An error within an update by the ECDIS provider could impact vessel systems in a similar way. Varying the narrative to the scenario may change the scenario loss, particularly in relation to the application of exclusions on standard polices, should there be no intent to do harm. The CrowdStrike-Microsoft defender outage was an example of service provider error resulting in loss of systems.

4. Cases

Source: Lloyd's

The below table includes a list of historical cyber events in chronological order. With the exception of NotPetya, none of these events led to a cyber catastrophe, however, these were all near misses.

Year	Event	Impact
1988	Morris Worm	An accidental software bug caused a computer worm to spread rapidly, crippling tens of thousands of computers and forcing important institutions to disconnect from the internet.
1999	Melissa	Email servers at corporations and government agencies worldwide became overloaded, and some had to be shut down entirely, including at Microsoft.
2000	ILOVEYOU	Disrupted the operations of businesses and government agencies including Ford, Merrill Lynch, the Pentagon and the British Parliament. The attack affected the confidentiality, integrity and availability of the machines.
2001	Code Red	Attacked web servers around the world and caused defacement and denial of service. The attack affected the availability and integrity of the machines.
2002	Internet Root Server Attack	A coordinated attack that disabled nine of 13 root servers running the internet's Domain Name System (DNS). One expert believes "it [was] clearly done with the intent to cripple or shutdown the internet".
2003	SQL Slammer	Worm caused tens of thousands of machines a denial of service on internet hosts and dramatically slowed general internet traffic, as well as disrupting access to most of the world's data query servers and networks. The attack affected the availability of the servers.
2008	Conficker	The worm attacked Windows machines slowing them down and disrupting their work and was present in systems owned by The Armed Forces of Germany, the UK, Ministry of Defence, the French Navy, hospitals and more. The attack affected the availability and integrity of the machines.
2016	Dyn DNS Provider Outage	The 2016 Dyn Cyber attack was a series of distributed denial-of-service attacks targeting systems operated by DNS provider Dyn from criminals in control of the Mirai botnet. The attack caused major internet platforms and services to be unavailable to large swathes of users in Europe and North America (including Twitter and PayPal).
2017	WannaCry	The attack targeted Windows machines, encrypting over 230,000 computers in more than 150 countries in a day. The attack demanded cryptocurrency in ransom to unlock the files. It affected the availability and confidentiality of the machines.
2017	NotPetya	The attack targeted Windows machines encrypting data. NotPetya heavily affected supply chain logistics companies such as the shipping giant Maersk, postal company FedEx and the Port of Rotterdam. The attack affected the availability and confidentiality of the machines. The NotPetya wiper, masquerading as ransomware, used a flaw in Ukrainian tax preparation software to spread the attack among international corporations, causing an estimated US$10 billion in damages.
2018	AWS Cloud Disruption Event	Parts of Amazon Web Services' US-East-1 region experienced approximately half an hour of downtime. Some customers' instances and data could not be restored because the hardware running them experienced complete failure. The attack affected the availability of the service.

4. Cases continued

Source: Lloyd's

Year	Event	Impact
2018	Microsoft Office 365 Outage in EU, Asia, US	Users from organisations all over the world, including the UK parliament, were unable to login to their email accounts or anything else hosted on Office 365, Microsoft's cloud computing service, for more than 15 hours. The attack affected the availability of the service.
2021	Kaseya	Using a zero-day vulnerability (unknown to the vendor) in a popular IT management tool, a criminal ransomware group infected between 800 and 1,500 businesses in one attack.
2024	Change Healthcare	Change Healthcare is a payment network utilised by various US-based hospitals and healthcare providers. On 21 February 2024, the parent company of Change Healthcare reported that the firm had suffered a ransomware incident which resulted in having to temporarily shut down operations. The ALPHV/BlackCat ransomware group claimed responsibility for the attack, claiming that it had stolen six terabytes of medical data. Healthcare providers across the US also reported disruption following the Change Healthcare payment network outage.
2024	Qilin	On 03 June 2024, ransomware hackers infiltrated the computer systems of Synnovis, which are used by two NHS trusts in London, and encrypted vital information making IT systems unusable. This resulted in the Russian cyber-criminal group sharing almost 400GB of private information on their darknet site and more than 3,000 hospital and GP appointments were disrupted by the attack.
2024	CrowdStrike	The recent IT outage cause by cybersecurity firm CrowdStrike crippled airlines, banking, healthcare, retail and many other industries. In total, about 8.5 million Windows devices were affected by the CrowdStrike-related outage that created an unwanted ripple effect across global supply chains.

5. References

United States Coast Guard. (August 2021). Cyber Strategic Outlook.
https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf

United States Coast Guard News. (22 February 2024). Executive Order Expands Coast Guard Authorities to Address Maritime Cyber Threats.
https://www.news.uscg.mil/maritime-commons/Article/3683564/executive-order-expands-coast-guard-authorities-to-address-maritime-cyber-threa/

United States Coast Guard. (2023). 2023 Cyber Trends and Insights in the Marine Environment.
https://www.uscg.mil/Portals/0/Images/cyber/CTIME_2023_FINAL.pdf

International Maritime Organization. (2024). Electronic Nautical Charts (ENC) and Electronic Chart Display and Information Systems (ECDIS).
https://www.imo.org/en/OurWork/Safety/Pages/ElectronicCharts.aspx

ener8. (01 January 2023). Merchant Fleet Infographic: 2023 Update.
https://www.ener8.com/merchant-fleet-infographic-2023/

International Ship Engineering Service Association (ISES). (10 December 2015). The majority of international fleet now fitted with ECDIS.
https://www.isesassociation.com/the-majority-of-international-fleet-now-fitted-with-ecdis/

UK Hydrographic Office (UKHO). (13 December 2023). Safe, efficient, and trusted digital navigation for mariners.
https://ukhodigital.blog.gov.uk/2023/12/13/safe-efficient-and-trusted-digital-navigation-for-mariners/

Admiralty. The UKHO supports digital solutions for vessels requiring non-ECDIS navigation. (16 November 2023).
https://www.admiralty.co.uk/sunsetting-paper-charts

International Monetary Fund. (16 April 2024). Global Financial Stability Report 2024.
https://www.imf.org/en/publications/gfsr

International Maritime Organization. (2024). Guidelines on Maritime Cyber Risk Management.
https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

6. Acknowledgements

Contributors

Lloyd’s Market Association’s Cyber Risk Strategy Group:

Patrick Bradley, Head of Non-Property Exposure Management
Tokio Marine Kiln

Ida Celentano, Executive, Technical Underwriting
Lloyd’s Market Association

Stephen Gibson, Casualty and Cyber Exposure Manager
AXIS Capital

Andrew Johns, Head of Reporting, Casualty and Cyber Risk Management
AXA XL

Dora Koutsoukou, Global Head of Cyber Risk Management
Global Risk Solutions, Liberty Mutual Insurance

Thomas Ledger, Head of Cyber Exposure Management
Hiscox

Kelly Malynn, Committee Chair, LMA’s Cyber Risk Strategy Group
and Underwriting Product Leader for Cyber Physical Damage M.A.P
Beazley

Chris Mather, Senior Executive, Technical Underwriting
Lloyd’s Market Association

Jennifer Thomlinson, Actuarial Head of Underwriting
Open Market, Brit Insurance

Other contributors:

David Baxter, VP, Risk Oversight Analytics
RenaissanceRe

Peter Hacker, Cybersecurity Expert
Founder and CEO Distinction.Global

Saheel Master, Former Group Head of Risk Analytics
IQUW

Andrew Wills, Cyber Pricing Analytics Actuary
AXIS Capital

lmalloyds.com

@LMAupdates   Lloyd's Market Association

Disclaimer
This document or presentation and all of its contents (collectively, the "Document") were intended for general informational purposes only. This Document is intended only for the designated recipient to whom it was originally delivered by Lloyd's Market Association ("LMA") and any other recipient to whose delivery LMA consents in writing (each, a "Recipient"). This Document is strictly confidential, and no Recipient shall reproduce this Document (in whole or part) or disclose, provide or make available this Document, or any portion or summary hereof, to any third party without the express written consent of LMA. This Document is made available on an "as is" basis, and LMA does not make any representation or warranty of any kind (whether express or implied), including without limitation in respect of the accuracy, completeness, timeliness, or sufficiency of the Document. This Document is not intended, nor shall it be considered, construed or deemed, as (1) an offer to sell or a solicitation of an offer to buy any security or any other financial product or asset, (2) an offer, solicitation, confirmation or any other basis to engage or effect in any transaction or contract (in respect of a security, financial product or otherwise), or (3) a statement of fact, advice or opinion by LMA or their directors, officers, employees, or representatives.