LLOYD'S

ABI

Components of a major cyber event:

a (re)insurance approach

November 2024

Table of Contents

Acknowledgements 3

How this paper can be used 4

Forewords 5

Executive Summary 6

Introduction to cyber risk 7

Who
Component 1: Attribution 8

What
Component 2: Cause of loss 12

Where
Component 3: Footprint 14

When
Component 4: Start and duration 17

How
Component 5: Spreading mechanism 20

Why
Component 6: Motive 24

Impact
Component 7: Monetary loss 25

Conclusion 28

Glossary of technical cyber terms 30

Acknowledgements

This paper has been produced as an artifact of the ABI Lloyd's Cyber Working Group.

This paper has benefitted significantly from inputs and comments from the members and affiliates of the ABI Lloyd's Cyber Working Group. Special thanks go to:

- Adam Banas, Gallagher Re
- Darren Gatcum, AXIS Capital
- Fraser Barr, Aon
- Geraldine Kearney and Victoria Häberle, Munich Re
- Glyn Thoms, Willis Towers Watson
- Henry Skeoch, Beazley
- Jacqueline Yeo, Lockton Re
- Lucy Fraser, Association of British Insurers
- Luke Foord-Kelcey, Howden Re
- Luke Fardell, Tokio Marine Kiln
- Matt Prevost, Chubb
- Samantha Dickens, Lloyd's
- Souki Chahid, Guy Carpenter
- Thomas Clayton, Zurich

We would also like to thank key reviewers including:

- The Lloyd's Market Association
- The ABI Cyber Insurance Committee
- Cyber AcuView, CyberCube, the Cyber Monitoring Centre, Cyence, Moody's
- Censys

While 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.

How this paper can be used

This paper can be used for enhancing awareness, education, and the development of risk appetite and (re)insurance solutions in managing cyber risk. While cyber risk practitioners may recognise the components of a major cyber event, this is the first time these elements have been brought together in a holistic, (re)insurance led way. The key stakeholder activity that this paper aims to support is outlined in the table below.

Key stakeholder	Supported activity
Modeler/Vendor	(Re)insurance led risk modelling
Wider interested party	Understanding of the market expertise
Consumer/Insured	Confidence in protection
Risk Manager	Enhanced and incentivised risk management chain
Exposure Manager	Risk tolerance setting
Capital Assessor	Capital requirement evaluation and clear allocation
Investor	Confident investment
Insurer	Coverage design
Reinsurer/ILS/IWS	Treaty performance and primary insurer evaluation

While the paper does not outline individual market approaches, it is intended to encourage readers to explore the market and wider topics further.

A glossary of technical cyber terms is provided at the end of the paper. Typical modelling input variables are also described in tables throughout. It is important to consider their relevance and certainty when analysing a specific major event. For instance:

- Determining who is responsible, or why a major cyber event happened can be challenging, however these questions are essential during loss assessments.
- Not all the typical components of a major cyber event apply to every modelled scenario. For example, including a malicious spreading mechanism in a model of a non-malicious event can skew the outputs.
- The more detailed the scenario description or modelled variables are, the less likely that exact event is to occur, potentially creating a false sense of confidence.

Forewords

Rachel Turk,
Chief Underwriting Officer at Lloyd's

Cyber risk is one of the most complex and critical challenges facing national security and businesses today. Not only is its pace of change and technological sophistication almost unmatched by other risks, it's at the intersection of sectors and societies across the globe.

At Lloyd's, Cyber is the fastest growing class of business – with over a fifth of global cyber insurance being placed here. The proliferation of cyber threats has necessitated the development of risk management strategies, particularly in defining what constitutes a "major cyber event."

Highlighting the importance of a better shared understanding of the approaches to defining a major cyber event is crucial for quantifying risks and for developing risk mitigation strategies. It also facilitates better communication and collaboration among insurers, insured entities, customers, third party security services, and regulatory bodies.

As the digital landscape continues to evolve, so too must our approach toward understanding and managing cyber risks. This paper seeks to contribute to the ongoing dialogue by proposing a robust framework for defining major cyber events, ultimately enhancing the resilience of the insurance industry in the face of ever-growing cyber threats.

Mervyn Skeet,
Director of General Insurance Policy at the ABI

The insurance industry has always had one eye on the future. As cyber risks become a more frequent part of our daily lives, we can see both threats and opportunities in the days and years ahead. The rules of cyber are still being defined, however the businesses of today need to take control and adapt as they evolve.

As it stands, businesses are grappling with a lack of awareness and readiness around cyber and the absence of standardised good practice or resourcing.

The challenges they face are significant, however this is where our industry, being at the forefront of understanding cyber risk, has a pivotal role to play. Together we can support customers and businesses amidst the uncertainty and help them better protect themselves from cyber-attacks.

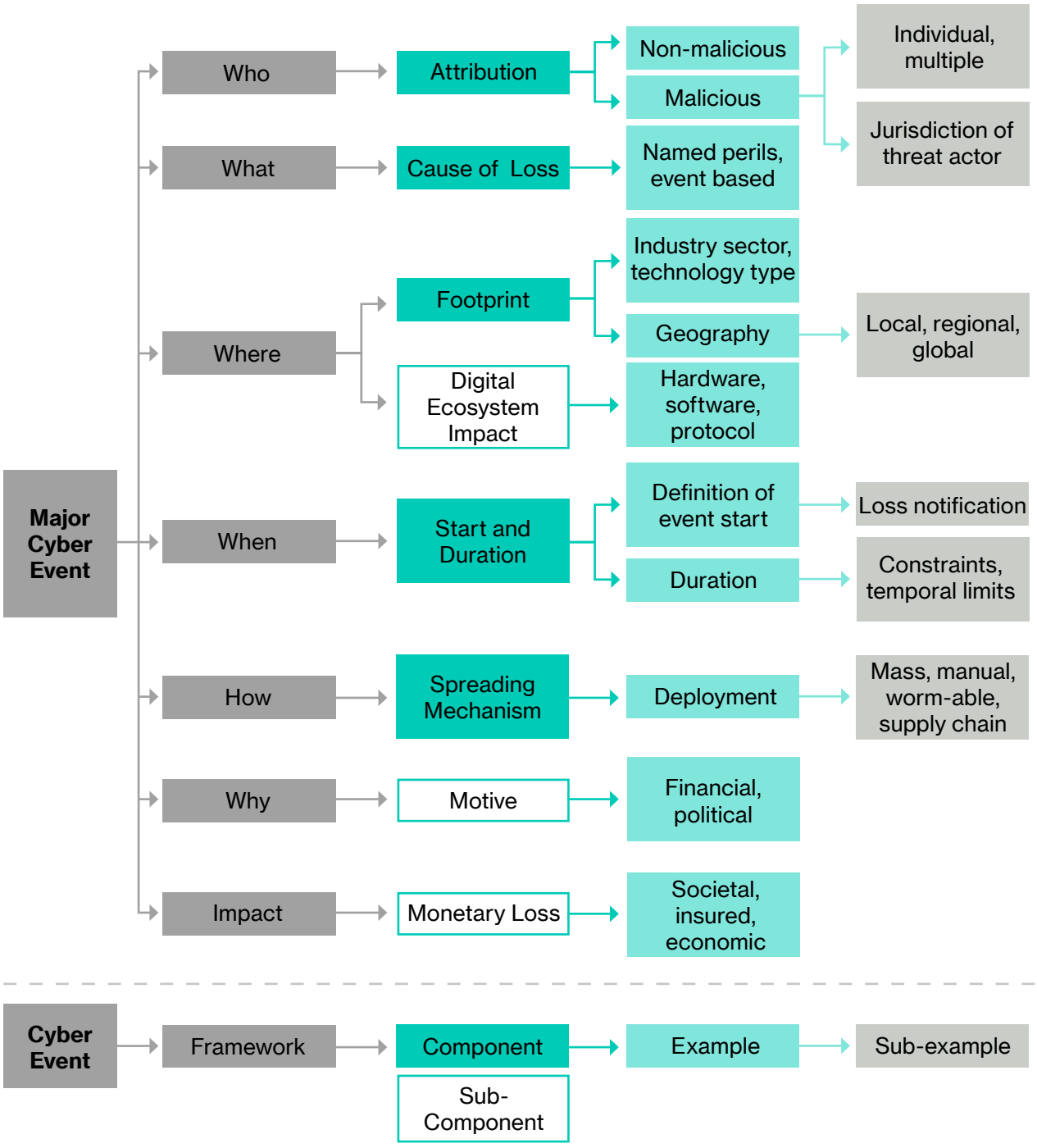
Insurance and security are key components of any strategy to mitigate cyber risks, however the scale of the threat is such that some events could dwarf the industry's ability to respond. The defence against cyber-crime cannot solely be insurance, we have to collaborate.

That is why we are also working with government, law enforcement, and other stakeholders to consider how to best address the threat and help to build resilience, contributing our knowledge and experience.

Executive Summary

This paper seeks to outline the key (re)insurance components for a consistent framework to define a major cyber event.

The diagram outlined below provides a visual representation of the framework. Breaking down the event into distinct elements – who (attribution), what (cause of loss), where (footprint and digital ecosystem impacts), when (start and duration), how (spreading mechanism), why (motive), and impact (monetary loss) – ensures comprehensive consideration of the critical aspects. This holistic perspective is vital for grasping the full scope of a major cyber event, facilitating clear analysis and communication among stakeholders, and ultimately enhancing resilience through better coordination.



(Re)insurers and partners can use this set of components to methodically analyse real or simulated insurance losses, which in turn may assist them in defining their risk appetite, in line with their commercial approaches. For example, the components could be used to communicate likely exposure to an event such as a widespread Operating System (e.g., Windows) outage.

This paper is an artifact of the ABI Lloyd's Cyber Working Group, made up of senior cyber (re)insurance leaders. It represents a collaborative effort, compatible with the diverse and innovative commercial approaches in the market. The insights which informed this paper are a result of research studies, modelling assessments, and thorough discussions with cyber professionals from across the cyber market.

Introduction to cyber risk

Cyber risk is a distinct and relatively new peril with the potential for outsized impacts. Major cyber events can affect vast numbers of people across geographical boundaries, disrupt state functions, cause significant operational disturbance, property damage, and even loss of life.

Cyber events often lack a clear beginning, end, or rational progression, spreading unpredictably from one system to another. The outcomes of these events can vary greatly, depending on the quality of the defence, response, and recovery measures in place, as well as human actions within these man-made systems.

Despite the increasing risk, as global dependence on technology grows, there is no comprehensive global definition of a major cyber event. Even governments struggle to determine which sort of events are large enough to fall within the national interest and thus under government responsibility. This is partly due to there being relatively few historic major cyber events upon which to base decisions.

Within the insurance industry, the absence of historical events can create uncertainty around policy coverage and setting outer boundaries for aggregating events. Consequently, components of cyber risk may be approached in isolation, without the benefit of a combined and collective context throughout the risk management chain, or an understanding of their relationship with adjoining issues. This complicates efforts to model, monitor, and transfer risk.

To support these vital discussions, this paper aims to comprehensively explore the (re)insurance components involved in a major cyber event. This holistic (re)insurance view marks the first time the full range of components has been detailed.

Who

Component 1: Attribution

Who

Cyber is an emerging, dynamic, man-made risk, often driven by malicious motives. This presents new challenges in understanding accumulation potential and defining events. Component 1, Attribution, considers single or multiple malicious threat actors, and non-malicious events. Malicious actors can then be further subdivided into categories such as individual hackers, groups, or nation states.

Component 1: Attribution

Attribution refers to identifying the responsible party, or parties behind a cyber-attack or malicious activity. Motive is closely linked to attribution and is discussed later in this paper, and can be a more subjective component.

Malicious
In malicious major events, there are significant considerations:

1. The process of trying to understand who is behind a cyber event(s) helps (re)insurers assess the source of loss, build up a threat intelligence picture, and understand the root cause of an event. Attribution may also be important for legal and coverage reasons. Where coverage is dependent on attribution, judicial or arbitral mechanisms may be required.
2. It is becoming more commonplace to identify individuals, entities, or sovereign states responsible for events. Intelligence regarding known threat actors is often available and agreed upon, and may include the typical motivations, attack style and targets of threat actor/s. It is especially true for significant events where multiple parties invest time and effort into uncovering the responsible actors.
3. Where attribution is not clear, there may be more easily identifiable information about a cyber event that can support a major cyber event definition, given that criminals are highly motivated to obscure who they are, and there are many ways they can hide. They might, for example, use proxies, advanced weapons such as drones, or malware false flags to remain unidentified. Different bodies might also attribute events to different actors.

These considerations in mind, there are also significant differences between events involving single vs multiple actors:

A single threat actor is the individual(s) or group who intentionally cause harm to digital devices, systems, or services. This can include individual hackers, organised groups, or nation-states. Examples of complications include:

- Different insureds or other groups may attribute the loss to different actors.
- There is potential for loss amplification if insureds assume the actor in the news for a major event is the same one that affected them, especially when state activity is suspected.
- Public narratives may exaggerate a threat actor or system vulnerability. Cyber-attacks are often described as targeting one specific entity, whereas in reality, criminal groups might be scanning many internet-facing infrastructures/businesses for vulnerabilities.

Multiple threat actors are especially likely in a 3rd or 4th party attack. For example:

- In a ransomware as a service (RaaS) attack, multiple threat actors come together creating a service supply chain of criminal activity, one compromising the victim, another negotiating a ransom demand, etc.
- It may not be possible to identify if there is more than one threat actor behind an attack (e.g., a criminal gang sponsored by a state).
- If a vulnerability becomes public knowledge and several threat actors exploit it in the same time period, (re)insurance losses might either be split by threat actor or alternatively accumulated:
    - Example 1: CVE-2022-47986 was exploited by both ransomware groups and Iranian state sponsored threat actors. If exploits from more than one threat actor are chained together the attribution may become highly challenging.

- Example 2: CVE-2023-40044 came under attack via multiple exploit chains, including an attempted ransomware deployment. If parts of the attack chain had been re-used from a different threat actor, that may impact attribution.

Non-malicious
Before the CrowdStrike event, discussion about major cyber events focused primarily on malicious cyber-attacks. With its brief downtime, CrowdStrike may support a modelling assumption that non-malicious attacks are comparatively less of a consideration for tail losses than malicious. However, significant losses can also arise from non-malicious events, such as via regulatory actions.

Instances involving the Biometric Information Privacy Act (BIPA) and Meta Pixel have resulted in significant 3rd party claims. Even though the actor is non-malicious, understanding who bears the ultimate responsibility for the loss in these events may be key for defining a major cyber event and the underlying (re)insurance contract.

To give some examples of non-malicious events, in 2023 Britain's National Air Traffic Services (NATS) experienced three days of chaos after a flight plan with bad data allegedly crashed their software. The same flight plan was then loaded into the backup software, allegedly exacerbating the problem. Furthermore, notable non-malicious outages occurred in 2020 and 2021, where prolonged system down-time was recorded for Cloudflare and Facebook, respectively. Another notable non-malicious outage was the 2021 Fastly incident, caused by a dormant bug introduced by a customer.

Potential additional concerns may include mergers and acquisitions (M&As) of service providers leading to corporate memory loss or faulty onboarding, and the hypothetical AI “paperclip problem”, where non-malicious code, if not correctly parametrised, could cause significant disruption.

Finally, a system failure at a large IT vendor could cause widespread market losses. However, it’s important to consider that failure of a smaller, less-resourced IT vendor serving a specific industry or region is likely to occur more frequently.

Attribution, applied

CrowdStrike: The cause of loss was identified very quickly in this event as non-malicious and this influenced the remediation activity and recovery. Most companies recovered swiftly, however there may be some still struggling, for example due to more unique technology infrastructures in place.

NotPetya: The cause of loss was also known shortly after the event occurred, however the impact of this malicious attack continues to reverberate across the globe. For example, it impacted Merck.

Typical modelling input variables			Description
Who	Attribution	Type of actor	Informs motivation and objectives as well as Tactics, Techniques, and Procedures (TTPs). Can be malicious/non-malicious, single/multiple threat actors.
		Jurisdiction(s) of threat actor	Sources of malicious attacks may be cross-border and involve multiple jurisdictions, therefore using a single jurisdiction may not always make sense; jurisdiction is most relevant when considering nation-state originating attacks. It may be necessary to stipulate whether states outside the impacted state are excluded for coverage reasons.
		Total criminal groups	This number would include criminal, hacktivists, insiders, and all others in a series of events.
		Total nation state / state actor	A percentage of events that may be assigned to being of nation-state origin.

What

Component 2: Cause of loss

What

This section considers the role of traditional (re)insurance aggregation concepts in the cyber context, including reference to some practical examples of possible (re)insurance interpretations.

Technical features of a cyber event, upon which market approaches may be based, are also described throughout the paper to support understanding of cause of loss (for example in the glossary, and application tables).

Component 2: Cause of loss

Extremely common in (re)insurance agreements, aggregation clauses are intended to allow or require multiple or separate losses to be treated as a single loss for the purposes of applying a deductible or limit. In structuring cyber event definitions, (re)insurers have sought to draw upon aggregation approaches traditionally used in the property and casualty context. The parties will stipulate a unifying factor, e.g. the same originating cause, event or named peril, for determining whether multiple individual losses stemming from the same "incident" can or must be aggregated.

While there have not been any decisions of the court yet in the cyber sphere, at the time of publishing this paper, the chosen aggregation mechanism will undoubtedly be a key component in determining the scope of a major cyber event for (re)insurance purposes. It is important to note that any aggregation analysis will remain a very fact and wording dependent exercise. A list of illustrative examples incorporated into wordings may be used to assist in interpretation.

Causation based language
Of the possible approaches, the causation-based or "common originating cause" language will, generally speaking, allow a wider range of losses to be aggregated compared to event based clauses. The use of "originating cause" aggregation language is interpreted under English law to be a conscious decision "to open up the widest possible search for a unifying factor for the losses that a party is seeking to aggregate"[1].

In practical cyber terms, a causation-based clause might allow for the aggregation of losses attributable to the same vulnerability, delivery mechanism or point of failure, even in circumstances where there have been subsequent intervening factors (e.g. human intervention to exploit a backdoor).

Event based language
By way of contrast, event based language, sometimes referred to as proximate cause language, is understood to be narrower than "originating cause" language. English courts have adopted a number of approaches for determining whether a particular incident can be considered an "event" or "occurrence" for the purposes of an aggregation clause. For example, in Caudle v Sharp (1995), the Court of Appeal decided that an "event" was "a more definite happening of something at some time" and only arises if:

- There is a common factor that can be properly described as an event;
- Which satisfied the test of causation;
- Which was not too remote for the purposes of the aggregation clause.

Subsequently, English courts started to apply the "unities" test of cause, locality, time, and the intentions of any human agents to determine whether the event is sufficiently connected to the loss(es) to allow for aggregation.

To apply event based language to the practical example of a widespread malware attack or data breach, losses could be aggregated if they arise from one identifiable incident. However, in a software supply chain attack where malware is delivered to install backdoors to carry out further activities, event based causation language might prevent aggregation of losses if individual human intervention is required every time to exploit a backdoor.

1. Lord Mustill, AXA Reinsurance (UK) plc v Field [1996] 1 WLR 1026

Named perils
Named perils language is understood to be even narrower than event based language, as it delineates what is constituted as an event based on forecasts rather than actual results or “underlying definitions”. In a cyber insurance context, this approach could outline specific triggers for coverage.

For example, a supply chain attack impacting multiple organisations due to a common software vulnerability could be aggregated under a "Software Supply Chain Event" peril. This type of named perils clause allows for a greater degree of control over what is covered, limiting ambiguity in major cyber incidents.

Cause of loss, applied

Typical modelling input variables			Description
What	**Cause of Loss**	Can the cause of loss be determined (Y/N)?	Cause of loss, for example, may be split by software type and vulnerability (e.g., publicly facing vulnerabilities, cross-platform attacks, etc.) and captured explicitly. Event type may be assigned as a data breach (DB), targeted ransomware, or Distributed Denial of Service (DDoS). For a given catastrophe event, it may be Mass DB, Mass Ransomware, pay processor outage or service provider outage. It could be assigned as a common delivery mechanism or single point of failure (SPoF).

Where

Component 3: Footprint

Where

A cyber event might be described at a high level in terms of the digital ecosystem, geography, type of technology, or industry sector where it happened.

Component 3: Footprint

Footprint refers to the number of companies, risks or exposures affected by a major cyber event. It is especially important to consider the area of the digital ecosystem and the geography of where the event has taken place in order to establish the footprint. The types of technology and industry sector(s) where an event takes place are also significant considerations that support a better understanding of a major event; however, they are not as pertinent in establishing the footprint.

If one is focusing on insured companies only, one way to determine the footprint is to identify those insureds that have made a loss notification, however this can take time.

Geography
A major cyber event possesses the ability to spread across many organisations in various regions or territories, due to the way technological operations work and are globally interconnected. Major cyber events may be:

- Localised: Affecting several organisations in the same sector, area or both.
- Regional: Affecting a large proportion of organisations in a particular region e.g. regional cloud outage.
- Global: Affecting organisations across multiple regions and/or territories.

A further consideration is the location of threat actors and the geopolitical relations between states, as this can impact the way a malicious major event unfolds across geographies.

Digital ecosystem
Understanding the parts of the digital ecosystem that might be affected following a major cyber event will help understand the aggregation potential, exposures at risk and overall size of the event. This can also help mitigate the risk or take actions that might halt the spread and reduce losses.

The table below describes the digital ecosystem using common examples.

Targeted area of the digital ecosystem	Example
Hardware (Operational Technology (OT))	Successfully exploiting a widely used OT platform e.g. Tridium Niagara4 control system would have extensive implications.
Software (does not have to be internet facing to be compromised)	Obtaining access to channels of communication between the software product and vendor or other infrastructure, leading to remote command and control of the systems running the software.
Protocol	Over-consuming server resources. An attack against a popular encryption method could affect confidence in all software reliant on this technology, such as Secure Shell (SSH) or Transport Layer Security (TLS).
Supply Chain	Accessing systems via a non-direct route. The compromise of a key supplier network is used to pivot to trusted clients' networks. For intangible events this could be an attack against software code, and might be associated with a particular technology, which is embedded in the ultimate target operating system.
Critical Infrastructure	Data centres experiencing widespread outage following a failure of the electricity grid. This may not be covered, and is typically currently defined in policies by some form of critical infrastructure exclusion in line with prudential regulations. Specialist financing, local or international government intervention may be required here. Exclusions can be triggered by physical (potentially a natural catastrophe) or non-physical attack.

This table contains selected examples and is not exhaustive.

Footprint, discussion
Understanding the footprint of an event is crucial for accurately assessing whether it is a major event in a (re)insurance context. It has unique traits compared to other (re)insurance approaches of assessing frequency and severity of losses. The economic evaluation of major cyber events is that they are low frequency occurrences that could cause extreme losses.

However, not all major cyber events will have far-reaching footprints. Indeed, more frequent, minor cyber events may also incur similar, or even larger footprints. High frequency also does not imply a wide footprint, if the potential losses are not aggregable. For example, in the Log4j incident, there were a significant number of insurance claims notifications but ultimately not a large accumulation of claims.

Certainty of the footprint can be challenging, depending on the nature of the event. Where the accumulation point is a data breach or a single point of failure (SPoF) to which the loss can be directly attributed, calculating the footprint is objective. However, there may be more nuanced cases to consider such as distributed denial-of-service (DDoS) attacks, where threat actor attribution is complex. This is particularly significant if identification of a threat actor is being used as a footprint trigger, and some (re) insurance approaches require this identification to be performed at primary insurer level.

Further complexities include:

- **Long tail claims:** For example, claims relating to liability may mean that the timespan is elongated under which the full loss associated with a footprint of an event becomes apparent.
- **Indirect claims:** These may not be considered as part of the footprint of the same cyber event.
- **Common technology or SPoF:** The identification of a common SPoF does not guarantee an event qualifies as an accumulation event

Footprint, applied
HWL Elsworth: For HWL Elsworth, a large law firm out of Australia who was the subject of a data breach, the geography of their clients played a significant role in the nature of the event as there were many jurisdictional legislations in place.

CrowdStrike: CrowdStrike unfolded across different time zones, due to the global market reach of their services, and so geography may be a significant consideration when defining this event.

Typical modelling input variables			Description
What	Footprint	Total number of insureds using technology and the software type	This can be modelled on an exposure basis when modelling a breadth of events. Scanning tools can be used.
		Number likely to be directly impacted by event	Required.
		Indirect impacts leading to Contingent Business Interruption (CBI) losses	Only for cloud outages, CBI is considered (indirect impact to the companies due to lack of access to cloud servers).
	Digital Ecosystem (subcomponent)	Type of technology impacted	A particular software, or a particular provider of network services. Ability to understand the “materiality” of certain provided services.
		Critical infrastructure (not explicitly included)	Industry-specific vulnerability—such as vulnerability facing utilities or energy sector entities—are implicitly considered. It provides information required to understand specific exclusions.
	Geography (subcomponent)	Location of event	Location of regional provider hubs, and location of impacted companies/the insured.

When

Component 4: Start and duration

When

Determining the start and duration of a major cyber event can be a challenge. A 24-hour IT outage has a shorter and clearer start time and duration than a widespread software attack on a vulnerability, or an issue that businesses take a long time to patch.

Component 4: Start and duration

There are formal approaches to defining the start and duration of an event:

- (Re)insurance approaches set loss tolerances within a fixed period of time.
- Information security methodologies such as MITRE ATT&CK[2] and the cyber kill-chain introduce more details and granularity.
- External bodies may independently announce their interpretation of the start and duration of a major cyber event.

(Re)insurers use factors such as incident response time, downtime, recovery time, and analysis of the attack's nature to gain a better view of when an event occurred and how long it lasted. This also draws upon other components, such as the Spreading Mechanism or Footprint.

(Re)insurance approach
A major cyber event can be defined by applying a formal start and duration in addition to other components, such as the number of insureds impacted, aggregation language used, or underlying reasons why losses occur such as threat actor or technology. However, the differing interpretations of start and duration may challenge (re)insurance approaches in some cases. There is a need for a consistent approach to ensure that losses are categorised and thus indemnified accordingly, and to support timely response and coverage under the policy terms.

The start of the event
The (re)insurance approach chooses a specific date from which to attach aggregated losses in accordance with their practices and appetite.

An event could begin when a threat actor or malicious code enters a system without causing disruption, when an attack is deployed or triggered, upon the insured's first discovery, or upon notification of a cyber-attack (which is typically when financial loss begins to manifest). The start date may also be placed at the discretion of the (re)insurer in order to maximise loss recovery.

For primary cover, upon discovering the malicious activity, the insured would be advised to notify it immediately to the insurer and seek support to remediate. If the loss materialises at a later date, the policy may treat the date of loss (DOL) as the date of notification.

The duration of the event
The (re)insurance approach to understanding event duration is similar across many insurance lines, typically allowing a 60, 90, or 120-day window for the aggregation of losses. However, it may take time to build awareness of who was impacted and how, as companies conduct due diligence and forensics. The notification process of multiple impacted parties can extend the time it takes to realise the event's impact.

2.

Start and duration, applied

MOVEit: If MOVEit is viewed as a single event a 60, 90, or 120 day reporting window is straightforward. However, MOVEit involved a data breach of a central database and many companies realised at different times that they were impacted.

CrowdStrike: This was an event with a comparatively more clearly known start and duration, based on the effect(s) of a specific technology error, and a record of who was using that technology.

Typical modelling input variables			Description
What	Duration	Total duration of event	Primary policy hourly waiting periods, caps and reporting periods.
		If partial restoration is completed	Relates to recovery time.
		Length of downtime per insured	Take into consideration Business Interruption (BI) durations by deriving a distribution around BI potential associated with the insured's size, industry and geography.
		Ability to apply hours clause	Applies to wait period deductible only.
		Event start	Approached using different methodologies.

How

Component 5: Spreading mechanism

How

Modern telemetry, endpoint detection, and response tools make it possible to see a cyber-attack 'make landfall' and track its movement, even if there can be challenges in fully understanding an event.

Component 5: Spreading mechanism

The spreading mechanism is the mechanism by which malicious files, code or activity spread in a cyber incident. There are several helpful outcomes to understanding how this happens in a major cyber event. This helps determine:

- The potential number of companies, geographies, and infrastructures that could be impacted and whether they were targeted or not.
- Whether individual losses are eligible for aggregation into an event. In some instances, any loss where malware was manually deployed may be deemed a single loss which is not eligible for aggregation.
- Whether there is contained spreading or whether the spread is rapid and extensive.
- Risk management capabilities, given that the mechanism of spreading malicious code can also be significantly linked to human behavioural response.

Forensic analysis of affected networks will, depending on the extent to which logs and evidence are kept and protected from the effects of the event, identify the initial access vector and identify the method that was utilised to spread from system to system. This can reveal more about the event, as well as its potential trajectory.

Defined spreading mechanisms
In a major cyber event, affecting numerous systems and networks, there are currently four main spreading mechanisms which are linked to the initial attack vector. They may support a 'defined peril' approach. It is important to note that there may also be other ways a cyber event can transpire, many probably currently unknown.

Manual deployment
This is the most common type of malware deployment. To date, it has been less likely to cause a major cyber event, unless the attack successfully targets a critical service which many separate networks and systems rely on. A threat actor manually deploys malicious files, code, or activity to the affected systems one by one. This can be a multi-step process of vulnerability exploitation followed by malware deployment and execution. There can be significant variability in this type of spreading mechanism. For example, differences in the exploitation mechanisms, the time taken between different stages of the attack, and the time taken to access distinct networks.

Mass deployment
This is the automated widespread distribution of malicious files, code, or activities. Mass deployment is accomplished by exploiting a common vulnerability or weakness that results in unauthorised access to assets (including malicious network access and or the resultant loss of network access). Such activities are marked by the rapid initial access affecting numerous distinct networks within a timeframe that would be otherwise improbable for a single threat actor or group. This type of attack may also use email as a vector to deliver the malicious effects.

Worm-able deployment
This is the deployment of malicious files or code which self-propagates. The worm usually moves to new systems using the same vulnerability. However, sometimes it uses different attack vectors/methods of entry. Forensic analysis can trace back the attack vector to other compromised networks or systems. The reverse engineering of the malware will also identify the traits of a worm-able piece of malicious code.

Supply chain deployment
This is the deployment of malicious code, files, or activity via a non-direct route, compromising a network's software, hardware, or protocols to get to another. There is usually a commonality in the initial attack vector that can be traced back across multiple distinct networks or systems.

Spreading mechanism, applied
This chart illustrates, at a high level, the point at which each attack method reaches its maximum effectiveness.

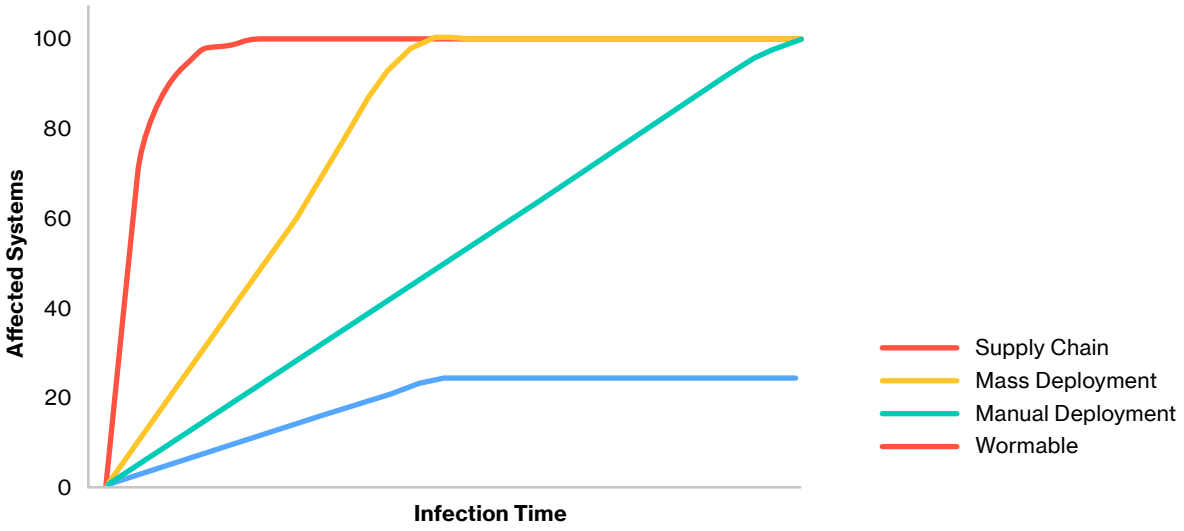


Figure 1: Known Malware/Malicious Spreading Mechanisms: Number of Affected Systems against Infection Time (Luke Fardell, TMK)

- Wormable attacks consistently increase in victims as the malicious files self-propagate from machine to machine.
- Mass deployment attacks start cautiously and once proven impactful are deployed at scale quickly reaching maximum effectiveness for the threat actor.
- Manual deployments are ineffective at scaled attacks and are often identified and mitigated against more quickly than they spread.
- Supply Chain attacks take full effect quickly once the distribution occurs.

Typical modelling input variables			Description
How	Spreading Mechanism	Manual deployment	Can be modelled as "bespoke" attacks
		Mass deployment	Catch-all term that considers all types of malware deployment mechanisms listed (wormable, supply chain, etc.)..

Why

Component 6: Motive

Why

The reason why an event occurs is closely linked to who is responsible /the attribution.

Component 6: Motive

Motive can have significant impacts on coverage where major cyber event definitions focus upon state backed and terrorist events. These events have the propensity to become highly complex.

When done correctly, attribution is factual, and evidence based, while assessing motive in a major event can be more subjective and judgement-based. For example, if a cyber operation is carried out by a state actor the motive can be subjective. Interpretations will vary by country and depend on sovereign response and wider geopolitics. An attack could also accidentally hit non-targeted entities outside the intended jurisdiction, in which case the motive (or lack thereof) may matter in a major cyber event definition.

Motive applied

NotPetya: This attack was specifically targeted at one nation, Ukraine, however there were widespread, unintended and severe impacts effecting non-Ukrainian targets globally.

Typical modelling input variables			Description
Why	Motive	Total accidental	Accidental (e.g., non-malicious) as a cause of loss can be captured for example, in Cloud Provider Failure Models. May be introduced as a cause of loss for malware/ransomware.
		Total malicious	Sum of the malicious actor subtypes (e.g., criminal, nation-state, hacktivist, etc.). This component is often involved indirectly under other components i.e. type of loss and attribution. The motive can aid event paths e.g. a ransom motive versus pure interruption defined uniquely.

Impact

Component 7: Monetary loss

Impact

Loss Impact is a financial measure used to determine the severity of a cyber event by comparing accumulated losses to a pre-determined threshold.

Component 7: Monetary loss

It might not go into a definition, however, once an event has been defined, understanding monetary loss will help to quantify the loss estimate, which will feed into models and risk appetite, and could subsequently help to classify whether the loss is significant enough to be considered a major cyber event. There are three key considerations.

Firstly, traditional information security approaches can be helpful in assessing losses. For example:

- In a data breach the financial impact depends on the type of data compromised. To understand this better, the traditional CIA approach can be used, to check if there was a loss of confidentiality, integrity, or availability of the data.
- In any cyber event, response time, downtime, and recovery time add helpful points of view from which to assess loss, with other considerations such as forensic investigation, legal expertise, and staff time included.

These factors contribute largely to contingent business interruption/business interruption insurance losses.

Monetary loss is especially relevant in a single risk context and can be taken at aggregate level to establish loss on one event.

Secondly, there are two types of monetary loss, which are insured and economic. There is merit in understanding and comparing both of them. In cyber events in which the insurance take up is low, the insured loss could be disproportionately small compared to the economic loss, and skew perceptions of the event. In this kind of low insured, high economic loss event, there may be higher volumes of claims and expectations of cover to factor in and so it can be important not to solely consider insured loss without factoring in economic loss.

Thirdly, while losses can increase as threat actors gain more control over their victims' systems, there can be component variations such as spreading mechanism, footprint, or the cause of loss that change the ultimate loss. These variations should be considered when applying the framework in this paper as a whole.

Insured loss
(Re)insurers will naturally be focused on the insured loss. This involves understanding the event, the subsequent insurance loss, and the overarching characterising components discussed in this paper. It involves understanding:

- **Impact on individual insured:** Provides better insights into loss severity or ultimate loss for (re) insurers. This information aids in modelling the severity of a major cyber event.
- **Loss impact characteristics:** Using the components in this framework can help set the outer boundaries for aggregating potentially small individual losses that are sufficiently connected in order to be included in the same event.
- **Threshold comparison:** Comparing the number of insured organisations that have been impacted with a pre-determined threshold can help determine if the loss is large enough to be classified as a major cyber event.

Economic loss
In contrast to insured loss, some would argue that the most straightforward threshold to define a major cyber event is economic loss, as it allows insured and non-insured major events to be measured and compared. For example, a hospital ransomware attack resulting in a fatality, with clear human impact, and a ransomware attack on a technology provider affecting thousands of companies, although very different, could both be evaluated on the same scale.

Monetary loss, applied

Entity Impacted & Measurement	Economic Loss	Insured Loss	Societal Disruption	Loss of Life
Colonial Pipeline	Significant	Cyber program Limit ($50m)	Minimal long term	None
Companies directly dependent on Colonial Pipeline	Minimal but unknowable	Minimal but unknowable absent specific tracking	None	None
Society at-large	Minimal but unknowable	Minimal but unknowable absent specific tracking	Significant short term	None

Colonial Pipeline: Understanding the loss can be challenging, it often takes time, and can vary depending on the type of loss being described. The table below compares Colonial Pipeline losses from the perspective of 3 different parties in order to demonstrate the complexity:

Typical modelling input variables			Description
Impact	Monetary Loss	Total insured loss available for each event	Required
		Sublimit considered in the insured loss calculation	Required
		Potential economic loss	Adds to further context

Colonial Pipeline: Understanding the loss can be challenging, it often takes time, and can vary depending on the type of loss being described. The table below compares Colonial Pipeline losses from the perspective of 3 different parties in order to demonstrate the complexity:Colonial Pipeline: Understanding the loss can be challenging, it often takes time, and can vary depending on the type of loss being described. The table below compares Colonial Pipeline losses from the perspective of 3 different parties in order to demonstrate the complexity:

Conclusion

Conclusion

As the landscape of cyber risk continually evolves, so too does the narrative surrounding it. The dynamic nature of cyber threats necessitates ongoing dialogue and adaptation. This paper has represented a snapshot in time within a broader, ongoing conversation about cyber risk management. By consolidating these insights, the aim has been to facilitate a deeper understanding and encourage collaborative efforts to address the ever-changing challenges in the cyber risk landscape.

In the (re)insurance context, defining a major cyber event requires a comprehensive understanding of its characterising components and their interpretation. This paper, developed through the collaborative efforts of Lloyd's and the ABI, has aimed to provide a robust framework for further work to identify, categorise, and define major cyber events. The paper has sought to assess, evaluate, and position clearer parameters around the consideration of cyber events with the potential to impact society, and by proxy the insurance industry, at scale. The hope is that this will support efforts to enable:

1. Increased coverage.
2. Consistent and confident investment of capital into the market.
3. Clear allocation of capital towards assumed risks.
4. Improved risk modelling methods in order to consider event loss amounts.
5. Enhanced and incentivised risk management.
6. Established, clear foundations to explore and structure complementary risk management and capital tools (e.g., risk pools, coinsurance, exclusions).

Ultimately, this paper has aimed to enhance the (re)insurance and partnered industries' ability to manage and mitigate cyber risks, supporting a more resilient digital environment. By identifying existing gaps and suggesting potential solutions for cyber modelling and market development, this paper has hopefully paved the way for a more informed and proactive approach to handling major cyber events.

Glossary

Glossary of technical cyber terms

Term	Definition
Accumulation Paths	The routes through which cyber risks can accumulate, affecting multiple systems or organisations simultaneously.
Actions on Objectives	The phase where threat actors act on their initial goals, such as exfiltrating data, encrypting data or destroying systems.
Advanced Weapons (e.g., drones)	Autonomous systems that can act as intelligent agents in cyberspace, executing cyber-attacks or defensive manoeuvres. They identify and exploit system vulnerabilities, particularly in networked environments.
Backbone	The backbone of a network is another name for the core infrastructure that supports a network. This can be physical equipment and or a collection of services.
Backdoor	A method that allows both authorised and unauthorised users to bypass normal security measures and gain high-level access (root access) to a computer system, network, or software application.
CDK	A company providing software solutions for the automotive industry. CDK suffered a ransomware attack in June 2024.
Change Healthcare	A healthcare technology company that provides data and analytics-driven solutions. They suffered a ransomware attack in February 2024.
Cloudflare	A company providing content delivery network (CDN) and cybersecurity services. Mostly known for their DDoS protection services.
Common Vulnerabilities and Exposures (CVE)	A list of publicly disclosed cybersecurity vulnerabilities.
Computer	An electronic device for storing and processing data, according to instructions given to it.
Corrupt	Data that has been altered or damaged, making it unusable.
Cross-Platform Attacks	Cyber-attacks that can target multiple operating systems or device types.
Cyber Incident Response	The process of detecting, responding to, and recovering from cyberattacks.
Cyber Kill-Chain Model	A framework that outlines the steps or phases involved in a cyber-attack, from initial reconnaissance to achieving the attacker's objectives.
Data Breach	The unauthorised acquisition or exposure of sensitive, protected, or confidential data.
Delivery Mechanism	The method by which a cyber-attack or malware reaches its target, such as phishing emails or infected downloads.
Denial of Service (DoS)	Attacks aimed at making a machine or network resource unavailable to users by overwhelming it with a flood of illegitimate requests.
Downtime	Length of operational disruption (period when a system or network is unavailable) suffered by the insured, potentially leading to revenue loss, customer trust erosion, and brand value decline.
DDoS (Distributed Denial of Service)	A type of DoS attack where multiple systems flood a target to disrupt service.
Encryption	The process of converting information or data into a code, especially to prevent unauthorised access. Usually, the data is protected with a key, passcode or physical token which is needed to reverse the encryption.
Endpoint Detection and Response (EDR)	Tools and solutions used to detect and respond to threats on endpoints like computers and mobile devices. EDR has many forms but typically uses proprietary installed software which is fed with the latest cyber threat intelligence signals to identify malicious files and behaviour.
Exception Errors	Errors that occur during the execution of a program, often leading to crashes or other issues. 'Exception' is a programming word for a disruption to ordinary flow.

Exfiltration	The unauthorised transfer of data from an organisation's systems to an external location controlled by the threat actor.
Exploits	Code or techniques used to take advantage of vulnerabilities in systems or programs.
Fastly Incident	A major internet outage in 2021 which was caused by a configuration error at the content delivery network provider Fastly.
Forensic Analysis	The process of examining digital evidence to understand the details and origin of a cyber-attack.
Human Intervention	When people actively take control or make decisions in response to a cyber incident, often to stop or contain an attack.
Lateral Movement	The technique used by attackers to move throughout a network to find and compromise additional systems or valuable information.
Log4j	A logging utility in Java that was found to have a critical vulnerability in 2021.
Malware	Software specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
Malware False Flags	Malicious software designed to mislead, making an attack appear to come from another source.
MetaPixel	A tracking tool created by Meta used to collect data on user interactions on websites. Primarily for advertising purposes.
MITRE ATT&CK	A comprehensive framework that categorises and describes the tactics, techniques, and procedures (TTPs) used by threat actors to achieve their objectives. It can be used to assess/model the probability of an attack successfully developing to the next phase.
Network	A group of interconnected computers and devices that can communicate with each other and share resources.
NotPetya	A destructive malware attack in 2017 that initially appeared to be ransomware but was designed to cause damage.
Operational Technology	Hardware and software that detects or causes changes through direct monitoring and control of physical devices. Devices such as thermostats, switches and network machinery are most common.
Outage	A temporary or prolonged disruption in service, affecting essential operations like payment processing or service provision.
Phishing	A fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity in electronic communication, most commonly in email.
Point of Failure	A component or system that, if it fails, can cause the entire system or network to fail and/or can cause cascading impacts on second-order users of that component or system.
Propagation	The spread of malware or other malicious activities within a network.
Protocol	A set of rules governing the exchange of data over a network. Such as the internet protocol (IP) which defines how routing and addressing data packets across a network happens.
Proxies	Servers or systems that act as intermediaries, masking the true location or identity of a user or device.
Ransomware	A type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
Ransomware as a Service (RaaS)	A business model where ransomware developers sell their malware to affiliates who then launch attacks.
Recovery Time	The time taken to restore a network to a fully functioning state following a cyber-attack.

Response Time	Duration required to respond to a cyber event, including cyber incident response (CIR), forensic investigations, breach response, legal support and payment of fines. This can depend on the insureds operating jurisdictions or laws around certain attacks, ransomware or data breach. CIR processes and technologies can increase cost; however they can also increase an organisation's detection and response capabilities, limit their exposure and prevent/reduce losses. CIR may reveal detailed information around the attack which will, in turn, enable (re)insurers to identify whether it relates to a major cyber event. It is also dependent on third parties and other considerations entirely outside of the control of the Insured. It does not link to BI loss, which is the primary driver of systemic loss.
Reverse Engineering Malware	The process of analysing malware to understand its behaviour and develop countermeasures.
Secure Shell (SSH)	A protocol for securely accessing network services over an unsecured network. SSH is most commonly used for administration of systems remotely.
Severity	The level of damage or disruption caused by a cyber-attack, often assessed based on factors such as data loss, system downtime, and financial impact.
Social Engineering	The psychological manipulation of individuals into performing actions or divulging confidential information.
Supply Chain	The network of suppliers and vendors that provide products and services to third parties.
System Destruction	The deliberate damage or destruction of computer systems and data, often to hinder recovery efforts or cause significant disruption.
Systemic Risk	Risks arising from interconnected networks, leading to widespread and rapid adverse events affecting multiple entities simultaneously.
Telemetry	The automated collection and transmission of data from remote sources. Typically, in cyber security it relates to the transmission of log information or other data points used to assess the health of a system.
Third-Party Tracking Tools	Tools used by external entities to track user behaviour on websites.
Tietoevry	A Finnish company offering IT services and software solutions. They suffered a ransomware attack in January 2024.
Transport Layer Security (TLS)	A protocol that ensures privacy between communicating applications and their users on the internet. Used in web browsing, email and online transactions.
Vulnerability, e.g. Publicly Facing	A security weakness in a system or program that can be exploited, especially when it is exposed to the internet or external users.
WannaCry	A ransomware attack that spread rapidly in 2017, affecting numerous organisations worldwide.
Worm-able	A characteristic of malware that allows it to spread automatically across networks and systems.

LLOYD'S

ABI

Instagram Lloyds of London
LinkedIn Lloyds of London
YouTube Lloyd's Insurance

X @Britishinsurers
LinkedIn linkedin.com/company/association-of-british-insurers
Web abi.org.uk