cmc
Cyber Monitoring Centre

CYBER MONITORING CENTRE

Event Categorisation Methodology

February 2025

Table of Contents

Introduction

The Cyber Monitoring Centre (CMC) has been established to provide consistent classification of UK cyber events that impact the UK. The CMC is an independent, non-profit organisation that uses an objective framework to assess the severity of major cyber events as they occur, categorising incidents on an easy-to-understand scale from one (least severe) to five (most severe).

The CMC category is calculated based on the number of UK organisations impacted and the financial impact of the event.

The assessment combines polling, technical indicators, incident data, and insights from those with firsthand knowledge of the event. The analysis is overseen and reviewed by a Technical Committee of leading cyber experts who then determine the event classification. The target timeframe to categorise an event is 30 days from the event being known, although in 2025 this may take longer.

This document describes the process and methodology that the CMC and the Technical Committee uses to classify events.

Event Assessment Process

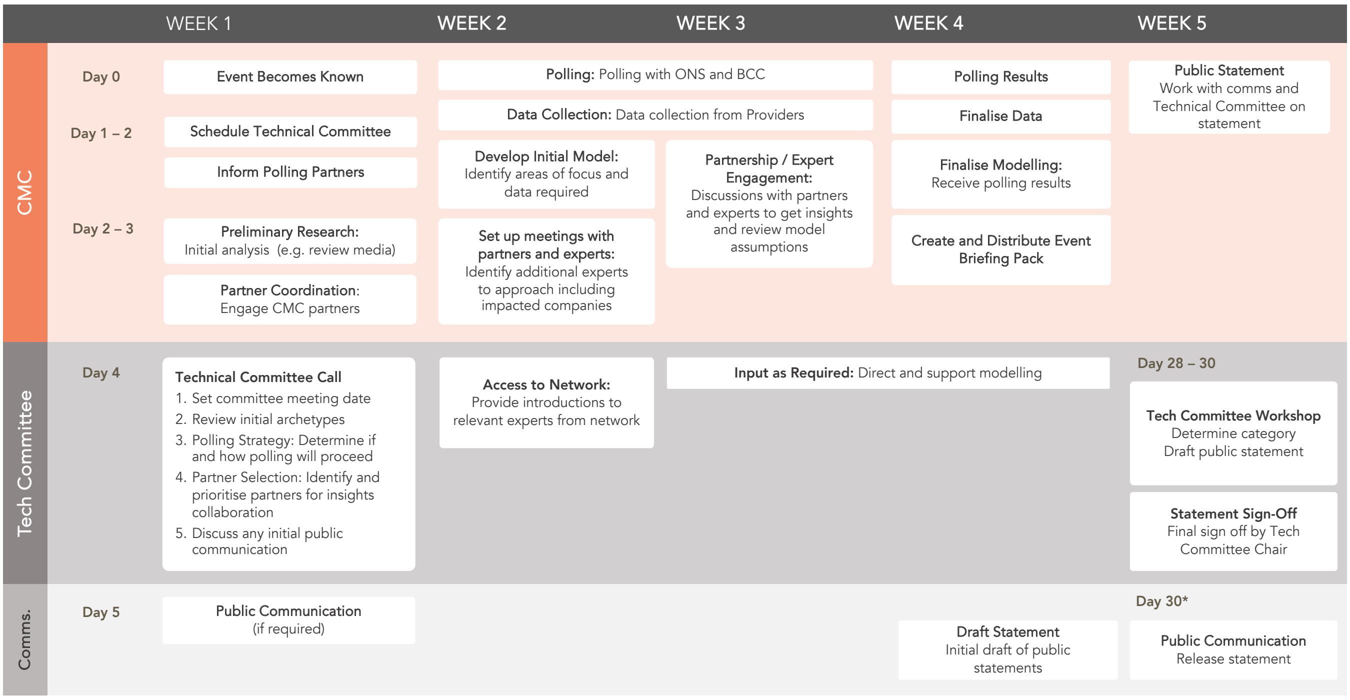
The event categorisation is determined by the CMC Technical Committee in line with the agreed methodology and definitions.

When an event occurs, the CMC team schedule a meeting with the Technical Committee to confirm the decision to proceed and get input into the assessment process. Then, depending on the nature of the event, the CMC team will work with polling companies, data providers, and other partners to collect and analyse the available event data.

The CMC team then provide an event briefing pack to the Technical Committee ahead of the Technical Committee half day workshop to discuss and challenge the assessment, and agree the event category. When the Technical Committee has categorised an event, this will be communicated in a public statement along with a brief statement about the event.

Exhibit 1 shows the timeline for event categorisation. It should be noted that the 30 day timeline is a target and not a commitment for 2025.

Exhibit 1: Events Assessment Timeline



WEEK 1 | WEEK 2 | WEEK 3 | WEEK 4 | WEEK 5

CMC

Day 0 – Event Becomes Known

Day 1 – 2 – Schedule Technical Committee

Inform Polling Partners

Day 2 – 3 – **Preliminary Research:** Initial analysis (e.g. review media)

Partner Coordination: Engage CMC partners

Polling: Polling with ONS and BCC

Data Collection: Data collection from Providers

Develop Initial Model: Identify areas of focus and data required

Set up meetings with partners and experts: Identify additional experts to approach including impacted companies

Partnership / Expert Engagement: Discussions with partners and experts to get insights and review model assumptions

Polling Results

Finalise Data

Finalise Modelling: Receive polling results

Create and Distribute Event Briefing Pack

Public Statement Work with comms and Technical Committee on statement

Tech Committee

Day 4 – **Technical Committee Call**

1. Set committee meeting date
2. Review initial archetypes
3. Polling Strategy: Determine if and how polling will proceed
4. Partner Selection: Identify and prioritise partners for insights collaboration
5. Discuss any initial public communication

Access to Network: Provide introductions to relevant experts from network

Input as Required: Direct and support modelling

Day 28 – 30 – **Tech Committee Workshop** Determine category Draft public statement

Statement Sign-Off Final sign off by Tech Committee Chair

Comms.

Day 5 – **Public Communication** (if required)

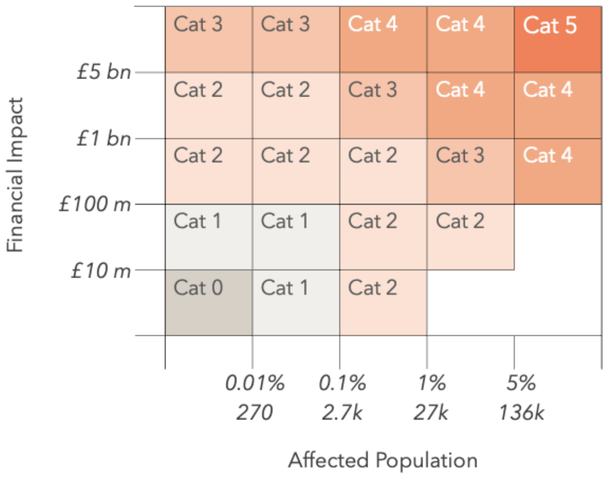
Draft Statement Initial draft of public statements

Day 30* – **Public Communication** Release statement

Definitions

Events are assessed using the CMC scale shown in Exhibit 2. The scale takes into account both the Financial Impact of an event and the percentage of organisations impacted or Affected Population. Events that have both a large Financial Impact and a large Affected Population have a higher rating on the scale.

Exhibit 2: The CMC Scale



Cat 3	Cat 3	Cat 4	Cat 4	Cat 5
Cat 2	Cat 2	Cat 3	Cat 4	Cat 4
Cat 2	Cat 2	Cat 2	Cat 3	Cat 4
Cat 1	Cat 1	Cat 2	Cat 2	
Cat 0	Cat 1	Cat 2		

The **Affected Population** is the number of organisations that have experienced a financial impact of £1k or greater to their UK operations as the result of a Cyber Event. Organisations include public organisations and registered companies. The total number of organisations in the UK is based on Office of National Statistics data. Included in the assessment are organisations that have suffered direct financial impact from a cyber event and those that have experienced a financial loss due to failure or disruption of a service provider, including but not limited to transport, hospitals, water, electricity provision, payment systems, cloud providers, and MSPs.

The **Financial Impact** is the loss to the Affected Population due to the Cyber Event. This includes losses due to business interruption, data restoration, incident response costs, extortion, and transfer of funds and includes downstream impacts of a cyber event. Costs due to liability, any fines or regulatory costs, apology payments, loss adjustment costs, and impacts to individuals are not included in the Financial Impact as these are not available in the immediate aftermath of an event and often these payments are a transfer of costs, rather than the true financial cost of an event.

The Impact to any single organisation is capped at £1bn, so that higher category events remain those that have significant impact to a number of organisations.

Data & Analytics

The CMC has a data driven approach, using a broad set of data sources to understand an event. This includes media scanning, bespoke polling, and partnerships with data providers. The data feeds the event analysis and modelling, and discussions are held with organisations that have insights into the event to capture any event specific factors or assumptions.

Polling

In 2024, the CMC carried out polling with the British Chambers of Commerce to understand the percentage of companies impacted by an event, the financial impact, the duration of impact, and cause of impact. The polling questions were included in surveys on other topics to reduce bias and provide unique insights into the impact of events that were not captured in media or other sources.

In 2025 we have extended the polling and survey approach:

1. We are now partnering with the Office of National Statistics to include polling questions in their fortnightly Business Insights and Conditions Survey (BICS), following a cyber event.
2. We have extended the relationship with the British Chambers of Commerce so that in addition to event polling we can survey a panel of cyber leads within companies, and industry specific panels, to understand the impact of an event.

Data

The CMC uses a combination of public and private data sources to assess events. Public data sources include media reports, NHS data, and data from the Office of National Statistics.

Data partnerships include Parametrix Analytics, a leading provider of cloud risk analytics services, who provide cloud monitoring and outage data, and Cirium, a leading provider of aviation analytics, to understand the impact on the UK aviation industry. More details on both partnerships are available on our website.

In addition we are developing a database of historical events and their impact for benchmarking, stress testing, and to help calibrate models.

Modelling

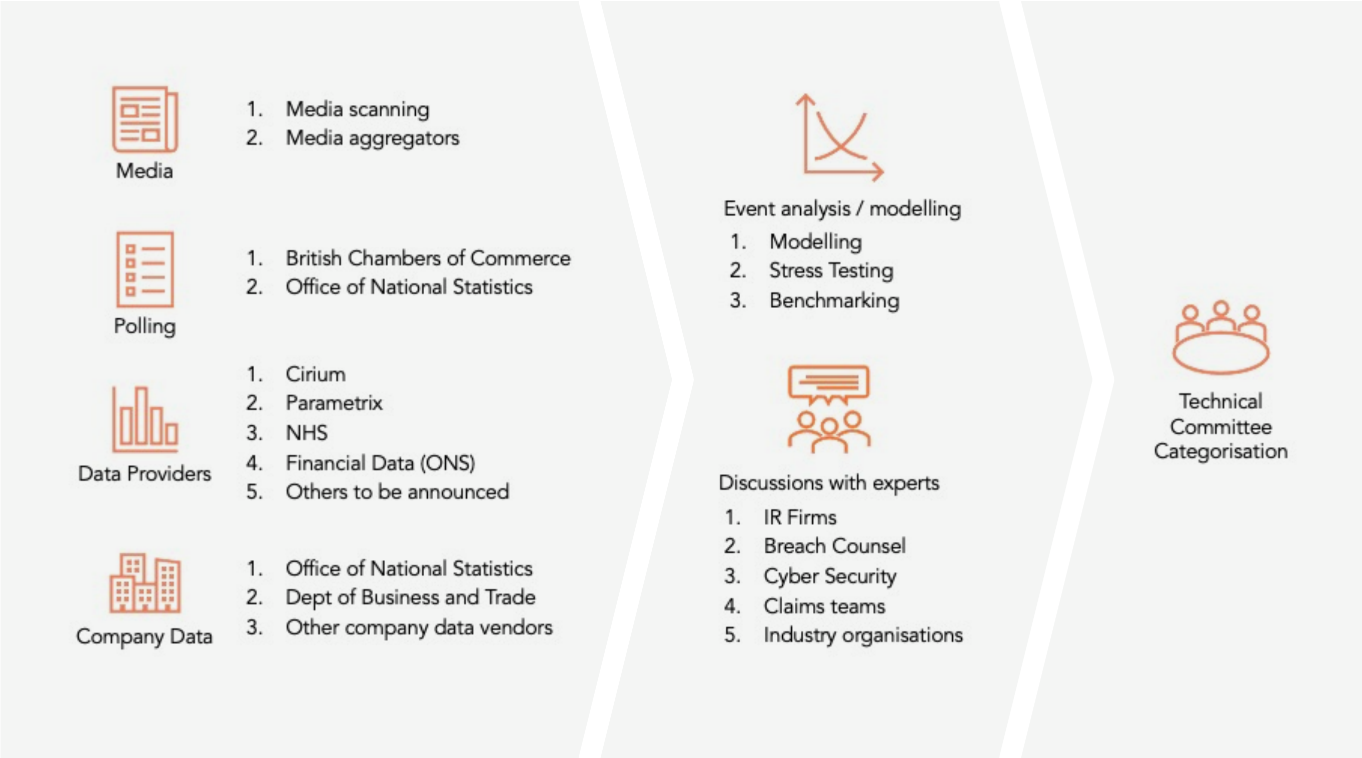
When an event occurs, we analyse the event and group the impacted organisations into those that can be modelled in a similar manner ("Archetypes"). We then collect available event data and model the financial impact to each Archetype. Through 2024 we developed models for aviation, healthcare (Synnovis event), and for widespread events (CrowdStrike event).

As new events occur, we use and recalibrate models that are applicable (for example, the healthcare modelling that was developed for Synnovis was reparameterised to assess the healthcare impact from CrowdStrike).

As we model an event, we also speak to companies and individuals who are involved, this includes contacting impacted organisations, and partners across incident response, breach lawyers, cyber security, insurance claims handlers, and industry associations.

The data and analytics process, including publicly available data and data providers that can be named, are shown in Exhibit 3.

Exhibit 3: Data & Analytics



Media
1. Media scanning
2. Media aggregators

Polling
1. British Chambers of Commerce
2. Office of National Statistics

Data Providers
1. Cirium
2. Parametrix
3. NHS
4. Financial Data (ONS)
5. Others to be announced

Company Data
1. Office of National Statistics
2. Dept of Business and Trade
3. Other company data vendors

Event analysis / modelling
1. Modelling
2. Stress Testing
3. Benchmarking

Discussions with experts
1. IR Firms
2. Breach Counsel
3. Cyber Security
4. Claims teams
5. Industry organisations

Technical Committee Categorisation

Categorising the Event

As well as providing expert input into the event assessment, the Technical Committee make the final decision on event categorisation.

The Committee is made up of leading experts with deep expertise in cyber security, quantitative risk modelling, cyber response, and cyber policy. In addition, the Technical Committee can request additional expert input where this will help with the event assessment. For example, for the analysis of Synnovis, the Technical Committee was joined by the Medical Director of a leading UK hospital. More detail on the Technical Committee can be found at **https://cybermonitoringcentre.com/technical-committee/**

The Technical Committee meet for half a day to agree the event category. In this meeting the Technical Committee review and challenge the event data, modelling, stress tests and benchmarking, listen to input from any external experts and discuss the categorisation, in line with the agreed methodology and definitions.

If an event is close to a categorisation boundary, the Technical Committee will determine the most appropriate category based on the data and insights available at the time of the meeting and their expert judgment. If the Technical Committee cannot reach a unanimous decision, there is an agreed mechanism for voting.

The CMC categorisation is based on the best available data, analysis, and judgment at the time of the Technical Committee meeting i.e. within 30 days of the event being known. The CMC continues to monitor the development of events that have been categorised to improve future modelling but no further public categorisation of an event occurs.