LLOYD'S

Lloyd's 2025 Market Wide Scenario Exercise Report

February 2026

LLOYD'S

2025 Market Wide Scenario Exercise (MWSE) – Executive Summary

Objective and report purpose
Lloyd's annual Market Wide Scenario Exercise (MWSE) enables managing agents to test their response to operational disruptions affecting core processes and Important Business Services (IBS), strengthening preparedness and resilience to severe but plausible events. This report summarises market responses across each phase of the 2025 exercise, highlighting areas of good practice, key insights and data, and lessons learnt.

Scenario overview
The 2025 MWSE simulated a broker outage triggered by a cyber incident compromising the broker's internal systems. To prevent propagation of malware, the broker was disconnected from Lloyd's Core Market Systems and from electronic placing platforms (e.g., CLASS, ECF, PPL). The disconnection disrupted claims processing, premium signings, and placement transactions, challenging participants to operate manual workaround to IBSs within impact tolerances. Participants were asked to coordinate across cyber security, business leadership, and communications teams - from the initial escalation of broker unresponsiveness through media speculation, informal transactional requests, and workaround management.

Summary of areas of good practice
Most managing agents highlighted that they would remain within impact tolerances during similar broker disruptions. Managing agents demonstrated risk-based, priority-driven decision making, particularly in cyber response and manual claims settlement, with clear prioritisation for vulnerable customers. Once the disruption was identified, operational concerns were escalated to leadership and IBS owners were engaged early and continuously. Broker reconnection was contingent on independent assurance and dual approvals from cyber security specialists and business leaders, reinforcing alignment across business and technology. As expected, agents looked to Lloyd's and the LMCTG for next-step guidance, with Velonetic supporting controlled operational activity and reconciliations, reflecting a preference for co-ordinated, market-level action. Cyber security containment measures were risk-based and consistent. Communications practices were disciplined: many treated social-media reports as credible until disproved, ensured accurate and consistent external messaging, and routed all incident communications through Communications, Legal and PR teams while instructing staff not to engage with online speculation.

Summary of key lessons learnt
The exercise highlighted that operational resilience across the market remains highly contingent on broker availability and the resilience of central processes, with many agents still orienting crisis planning and testing toward IT-vendor failures rather than third party outages such as distribution partners. Whilst, manual workarounds exist, they are difficult to scale during prolonged or multi-broker disruptions and they introduce reconciliation and duplicate payment risks. Foundational requirements such as documentation and staff training on manual workarounds was highlighted as an important 'back to basics' requirement. Separately, governance for disconnection and reconnection protocols is often under-specified and untested, compounded by limited visibility of system integrations and data flows which presented a risk to secure containment and recovery. As in previous tests, the exercise highlighted the interconnected nature of the market and agent's reliance on central guidance and the resilience of shared market services, reinforcing the need for continued collective work in creating consistent standards to drive timely, coordinated incident response.

LLOYD'S

Simulated Scenario Timeline (Monday 5th January 2026 – Monday 2nd February 2026)

PHASE 1 5th January	PHASE 2 6th January	PHASE 3 7th January	PHASE 4 8th – 18th January	PHASE 5 19th January	PHASE 6 2nd February
• **10:00** - The material broker is no longer responding to requests for outstanding claims and policy details.	• **06:00** - A national news agent has released a report that a Lloyd's broker has allegedly been targeted in a cyber-attack and these speculations suggest that the cause of the incident is related to unauthorised access into internal systems.	• **10:00** - The following morning, the participants have received text messages from broker colleagues which include operational requests such as rerouting transactional activities through personal email addresses.	• **13:00** - There are further speculations being spread across various social media platforms with unverified sources suggesting that the Lloyd's market participants may have been directly impacted by the cyber incident. The managing agents have been named in the alleged affected list.	• **15:00** - LMCTG provides confirmation that the incident has been resolved and the broker will be reconnected to the core market network through a strict protocol.	• **10:00** - Participants are presented with a series of questions following the remediation of the incident to determine whether their workarounds and contingency plans were effective to maintain IBS operations during the disruption.
• The material broker cannot complete actions on ECF, CLASS and placing platforms (e.g., Whitespace, PPL). • Although some brokers are in the Lloyd's building, they cannot access their internal systems. Daily premium processing has stalled due to the restricted access.	• Later that afternoon, LMCTG issues a market wide communication email to confirm that in collaboration with Velonetic and other market service providers, the broker's access to Lloyd's core market systems will be suspended until the incident has been resolved. • LMCTG has also advised the participants to conduct system health checks while the nature and extent of the incident remains under investigation.	• The text messages include operational requests to manually process and approve urgent claim submissions and payments through rerouting transactional activities to alternative email addresses.	• LMCTG have requested operational status updates and any signs of compromise or suspicious activity to be reported. • The broker remains disconnected from the market network as investigations continue. • A new email gateway has been established for the broker to communicate directly with managing agents via plain text emails, though documentation and images cannot be attached.	• Following a period of remediation Velonetic has authorised the broker's reconnection to the Lloyd's market systems as the cyber threat has now been neutralised and remediated. • Reconnection with the broker will be closely monitored for assurance of stability and complete removal of all malicious software.	• The participants were asked if they were able to continue operating their IBS within their impact tolerances during the disruption as well as any key lessons learned, and vulnerabilities from the disruption.

LLOYD'S

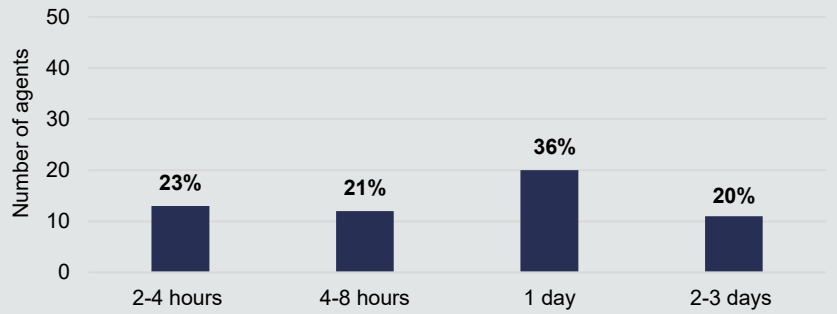
PHASE 1 - Scenario timeline: Monday 5th January 2026

The material broker is no longer responding to requests for outstanding claims and policy details. They cannot complete any actions on any market applications. Although some brokers are in the Lloyd's building, they cannot access the internal systems and this has led to daily premium processing being stalled.

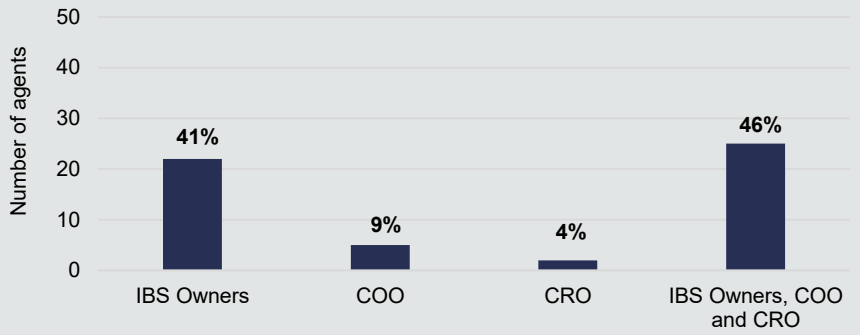
Phase 1 – Questions

1. After how long of the broker being unresponsive would you escalate and trigger an investigation?
2. At this stage, who internally would you escalate/ inform relating to this issue?
3. Based on what you know so far, would you convene your Crisis Response Team?
4. Which market associations or organisations would you reach out to externally?

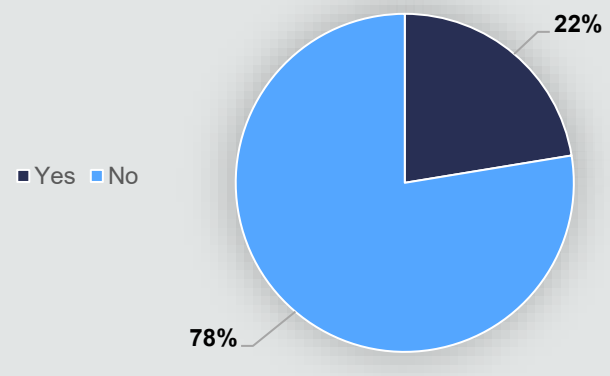
Summary of timescales for broker unresponsiveness escalation



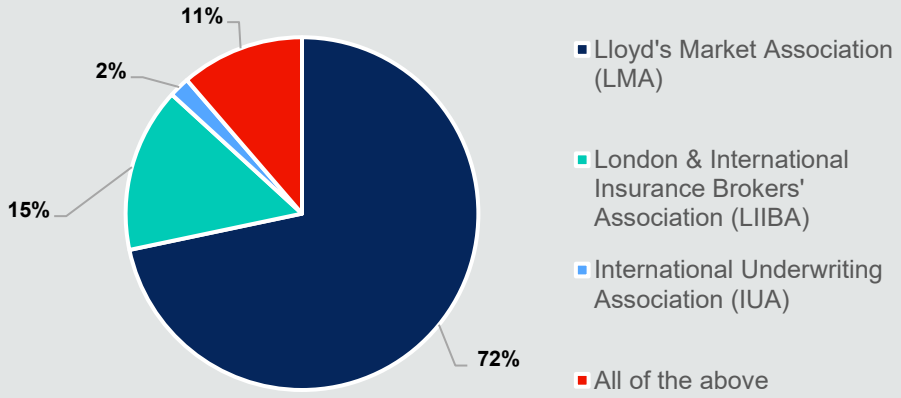
Summary of stakeholder escalation routes



The volume of participants that would convene their crisis response team at this stage of the disruption



Summary of market associations that would be contacted during the disruption



LLOYD'S

PHASE 2 - Scenario timeline: Tuesday 6th January 2026

A news outlet has reported that a Lloyd's broker has been targeted in a cyber-attack, the speculations suggest that the cause of the disruption is from unauthorised access into internal systems. LMCTG confirms that in collaboration with Velonetic, the broker's access to market systems will be suspended until the incident has been resolved. System health checks have been advised to the participants as the nature and extent of the incident remains under investigation.

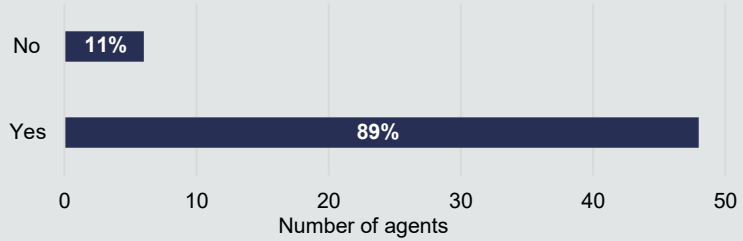
Phase 2 – Questions

1. How does your organisation assess the credibility of media reports about a cyber incident involving a key broker or other third party?
2. What actions, if any, would your cyber security team take at this stage?
3. What are your immediate operational priorities after LMCTG suspends broker access to Market Systems?
4. Would you disconnect the broker from your systems?
5. Is there a disconnection protocol in place?
6. Please can you describe your disconnection protocol or what steps you would take to disconnect from a third party? What risks or considerations would you have?
7. Which of the following best describes your contingency arrangements for broker-related disruptions?
8. What incident rating would you give this incident?
9. How do you interact with your IBS owners and what is the impact of this disruption on your Important Business Services?

Summary of approaches to media reports about the managing agent being impacted by the cyber incident

- 49% of participants have reported that they would treat media reports as credible until proven otherwise
- 22% of participants have reported that they rely on internal judgment and experience when assessing credibility of media reports
- 14% of participants report having a formal process for validating external reports
- 15% of participants reported that they would wait for confirmation from Lloyd's or other market agencies

Summary of responses on whether the participants would disconnect from the broker following confirmation of the cyber incident



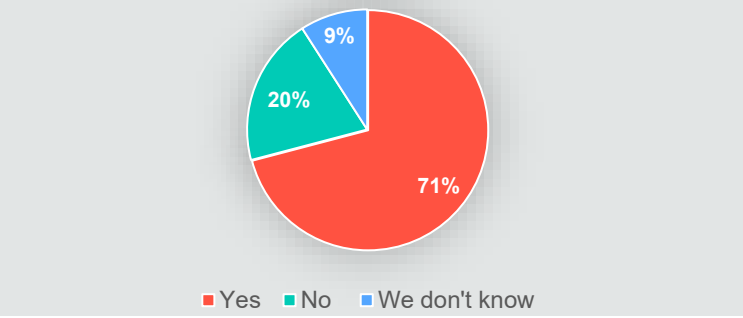
Areas of good practice relating to IBS owner engagement

- IBS owners conduct an impact assessment on their services and help prioritise vulnerable customers and time-sensitive transactions to avoid breaching impact tolerances
- IBS owners coordinate the implementation of documented workarounds such as manual processing, direct settlements or face-to-face trading ensuring alignment with regulatory obligations and internal governance
- IBS owners are involved from the start of the incident and kept updated throughout the disruption. Daily check-in and bridge calls with IBS owners
- IBS owners are integrated into Incident Management Teams to ensure visibility

Examples of good practice across agents' cyber security teams in response to speculations of potential wider market impact from the cyber incident

- Notification and coordination across senior leaders (CIO/CRO/COO) and liaising with Lloyd's/LMA and LIIBA and CISO groups to form a single, shared view of the incident to determine what's known or unknown from the cyber incident at this stage
- Heightened monitoring and scanning to rapidly rule out any contagion from the broker's compromised system through raising SIEM/SOAR posture for enhanced alert detection and tracking evidence of any unusual activity detected
- Quarantine and block broker emails/domains; identify integrations; disable broker single sign-on; revoke API keys; and implement firewall/IP blocks to prevent inbound and outbound connections

Percentage of respondents with a disconnection protocol



LLOYD'S

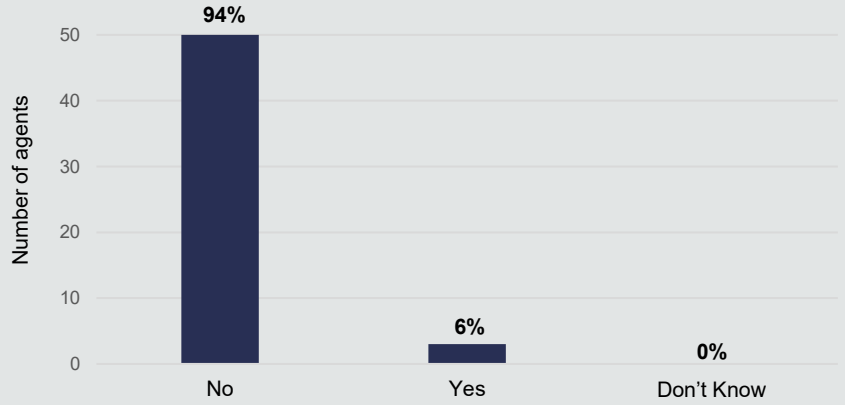
PHASE 3 - Scenario timeline: Wednesday 7th January 2026

Unverified transaction instructions have been provided by the broker from their mobile numbers and personal emails; these include operational requests to manually process and approve urgent claim payments through rerouting transactional activities to alternative email addresses.

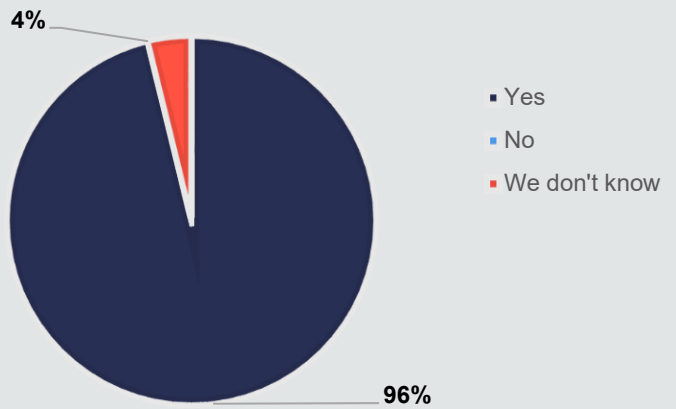
Phase 3 – Questions

1. Would your organisation act on the instructions provided via personal email addresses and numbers?
2. Are your workarounds/ contingency plans effective to appropriately manage IBS operations during this disruption?
3. Please describe your workarounds for managing in-flight transactions and claims during this disruption?
4. What assumptions are you making and what dependencies do you have to ensure that these workarounds are effective?

Percentage of managing agents that would act on the broker's instructions



The volume of responses that indicated whether existing workarounds and contingency plans would be effective during the disruption



Common workaround plans noted across the participants to manage IBS operations during the broker disruption

- 96% of participants noted that their Crisis Response Plans include scenarios relating to critical third parties
- 43% of responses mentioned that policyholders would be paid directly using Velonetic's 'direct settlement' routes or Lloyd's Urgent Settlement Guidance (USG) and LCCF procedures for urgent cases
- 39% of responses stated that they would revert to in-person meetings, paper files and wet stamps. All instructions would need to be validated by telephone or call-back to known contacts to mitigate phishing
- 31% of responses mentioned that where urgent the clients or insured would be contacted directly to progress payments and claim decisions, whilst trying to keep the broker in the loop
- Most responses have mentioned that they would focus on prioritising court-mandated payments and most vulnerable customers

LLOYD'S

PHASE 4 - Scenario timeline: Thursday 8th – 18th January 2026

Speculations have spread across social media platforms with unverified sources suggesting that Lloyd's participants may be directly impacted by the cyber incident. The managing agent has been named in the alleged affected list amongst other targets. LMCTG has requested updates on the managing agent's operational status and have advised for any signs of suspicious activity to be reported. The broker remains disconnected from the market network as investigations are ongoing. Although, the broker now has a new email gateway established which enables direct communication via plain text emails.

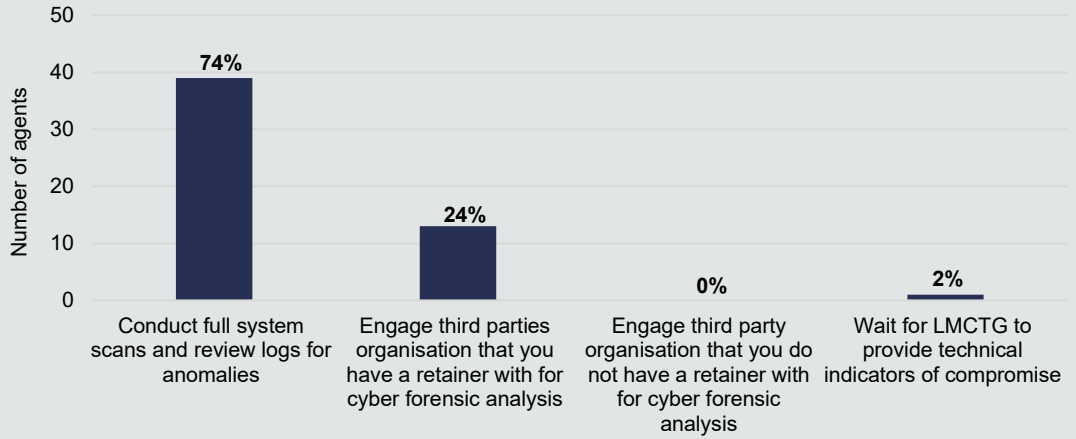
Phase 4 – Questions

1. How would your organisation respond to being named in unverified social media posts as affected by the cyber incident?
2. What steps would you take to confirm your operational status and check for suspicious activity?
3. Would you disconnect other managing agents named in the social media affected list from your systems?
4. Now that the broker has established plain text email capability from a new email gateway, would you rely on their instructions?
5. What evidence or information would you need from the broker to validate that a claim has been agreed by the lead before making urgent payments?
6. How would you manage internal awareness and staff communications across all levels

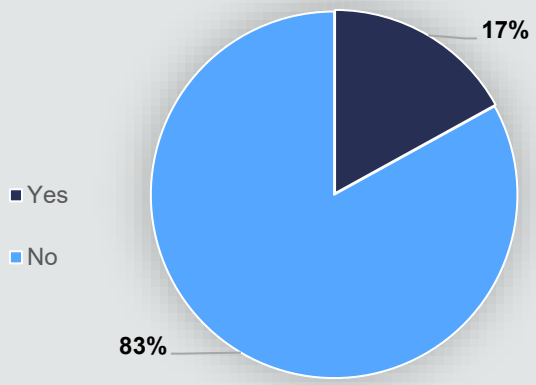
Good practices across participants in response to being mentioned in unverified speculations across social media platforms

- Engagement across Communications, Legal and PR teams to route and control any external messaging in response to the speculations of direct impact from the cyber incident
- No public statements will be released, all staff have been instructed to not provide any comments to the unverified reports
- Holding statements are prepared and pre-approved in case they are required

How participants would check their operational status for suspicious activity



Summary of responses on whether participants would rely on the broker instructions following the established email gateway



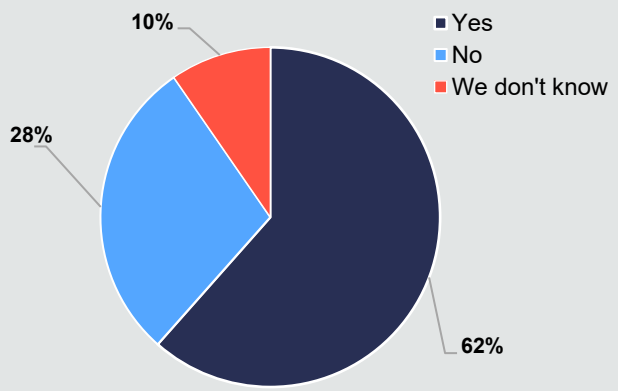
PHASE 5 - Scenario timeline: Monday 19th January 2026

LMCTG issues confirmation that the incident has been resolved. The broker will be reconnected to the core market network following a strict protocol. Following a period of remediation, Velonetic has authorised the broker's reconnection to the market systems after the threat has been neutralised and remediated. Reconnection will be closely monitored for assurance of stability and complete removal of all malicious software.

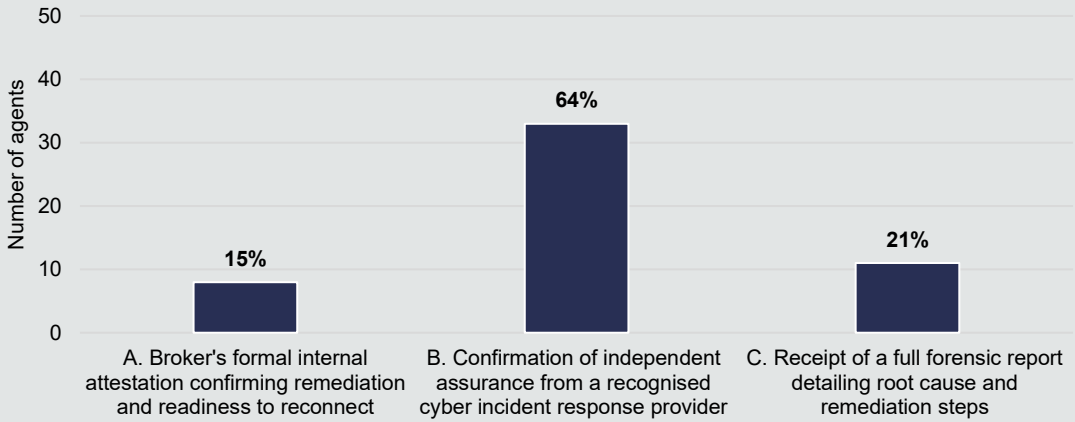
Phase 5 – Questions

1. What is your first action after LMCTG confirms the incident is resolved?
2. Do you have a reconnection protocol?
3. What assurance evidence would you consider sufficient before authorising reconnection?
4. What internal governance would you follow to authorise the reconnection?
5. What are your key considerations and risks during the reconnection?
6. Which technical steps should your organisation follow during the reconnection process?
7. Would you perform any regulatory notifications? If so, when would you notify?

Volume of participants that have a reconnection protocol



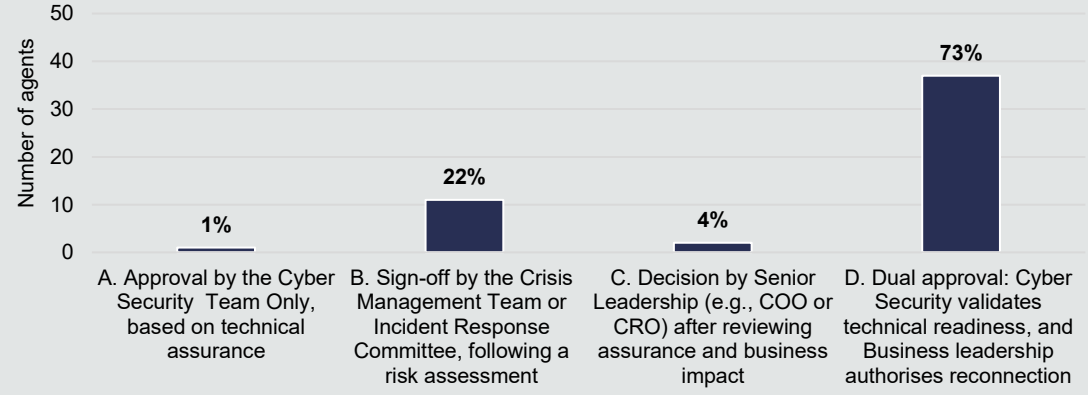
Assurance that the participants would want to see before reconnecting with the broker



Good practices across respondents' technical steps during the reconnection process

- Obtain independent assurance from Third-Party forensics, vulnerability scans or penetration tests
- Gradual reconnection in phases starting with low risks and non-critical systems
- Credential resets and access hygiene including resetting passwords, API keys, authentication tokens and enforce MFA (Multifactor Authentication)

Summary of respondents internal governance process to authorise reconnection



LLOYD'S

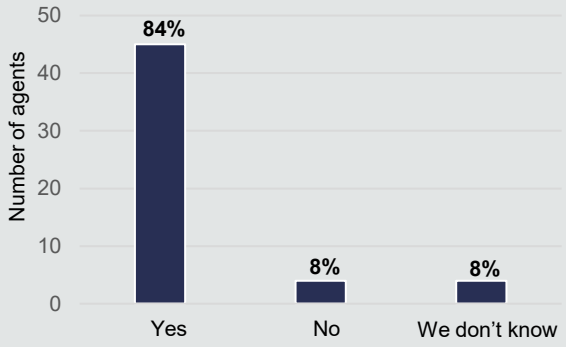
PHASE 6 - Scenario timeline: Monday 2nd February

Following the incident, participants were presented with a series of questions to explain if their workarounds and contingency plans were effective enough to maintain their Important Business Services within their Impact Tolerance levels. Participants were asked to share their key lessons learned as well as any identified vulnerabilities from the simulated disruption.

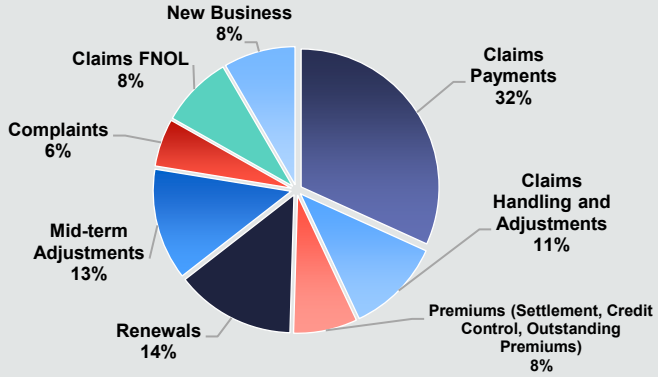
Phase 6 – Questions

1. Are your workarounds/ contingency plans effective to appropriately manage IBS operations during this disruption?
2. In this scenario, do you expect that you would remain within Impact Tolerances for your Important Business Services?
3. Please provide any comments relating to the effectiveness of your contingency plans and your ability to remain within impact tolerances for this scenario.
4. How will you manage the backlog of work to be processed as a result of this disruption?
5. What are your key lessons learnt, and vulnerabilities identified?
6. Do your Crisis Response plans include material third party failure scenarios?

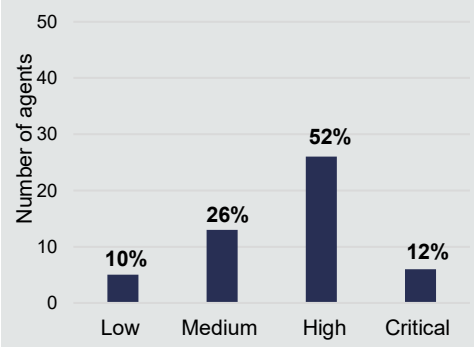
Managing agents that expect to remain within their impact tolerances throughout the disruption



Important Business Services that may be impacted by the broker disruption



Participants' severity scoring of the incident



Common practices across participants to manage the backlog of claims as a result of the disruption

- Triaging work based on risk and customer impact levels. Urgent claims and vulnerable customers would be prioritised as well as existing outstanding customer renewals, mid-term adjustments and endorsements
- Backlogs would be managed through scalable resourcing, redeploying internal staff who are cross-trained
- Processing will resume in a phased approach once the security assurance is confirmed to avoid overwhelming systems or team's post-reconnection
- Careful reconciliation of manual claims processed during the disruption by maintaining a log of manual claims, payments, endorsements and instructions in order to avoid duplication in payments, inaccurate non-cash bureau entries and ensure correct system updates

LLOYD'S

Areas of Good Practice

A summary of areas of good practice observed from participant responses

Risk-based decision making
Most managing agents highlighted risk-based and priority-driven decision making, including risk-based cyber measures and reliance on manual claims settlement with clear prioritisation (e.g., vulnerable customers, court-ordered payments).

Governance and escalation
Escalation timelines varied, reflecting different internal thresholds across the market. However, once the disruption was identified, managing agents typically escalated operational concerns to the COO/CIO and executive leadership, creating visibility across business and technology lines. Aligned to governance good practice, most managing agents noted that broker reconnection would only take place following independent assurance and dual internal approval from both cyber security technical experts and business leadership, reinforcing the alignment between business and technology that is critical in managing complex incidents.

Early and continuous engagement with IBS owners
85% of respondents indicated that they would escalate the incident to the IBS owners, who are embedded in Incident and Crisis Management protocols. Participants indicated that IBS owners would continuously assess performance and impact on the IBS, for example, by prioritising vulnerable customers and time-sensitive transactions and coordinate manual workarounds to avoid breaching impact tolerances. This is a strong indicator that Operational Resilience is effectively embedded across the business.

Cross-market engagement
Most respondents said that they would follow guidance from Lloyd's and the LMCTG to determine appropriate next steps and timing, with Velonetic supporting controlled operational activity and reconciliations. This reflects a preference for co-ordinated, market-level action rather than isolated responses. In addition, most managing agents would engage market associations (e.g., the LMA), reinforcing the market's inherent co-ordination which is critical given its interconnected nature.

Cyber security containment
Several firms emphasised risk-based disconnection protocols to avoid breaking in-flight transactions or corrupting data, balancing operational impact against cyber contagion risk.
A common set of disconnection actions was observed across participant responses, including immediately blocking all inbound and outbound email from the broker; redirecting broker messages to quarantine; disabling broker-associated user accounts; and resetting shared passwords and credentials. 80% of respondents referenced implementing network controls to safeguard internal systems and prevent malware spread. These controls included firewall rule changes to block IP ranges, blocking broker access to web platforms or portals, and disabling VPN/API links. Separately, over 75% indicated they would commit weeks of heightened surveillance using real-time SIEM (Security Information and Event Management) monitoring and additional alerts on privileged access or unusual behaviour. These measures demonstrate appropriate cyber hygiene practices.

Internal and external communications relating to social media speculation
In response to social media speculation, almost fifty percent of participants would treat such reports as credible until proven otherwise, reflecting a cautious stance that enables prudent risk management. Most participants demonstrated good practice by ensuring the accuracy and consistency of external messaging and by instructing staff not to engage with social media posts about the incident, routing all incident-related communications and announcements through Communications, Legal, and PR teams.

LLOYD'S

Key Lessons Learned

A summary of key challenges and lessons learnt, including examples of next steps identified

Broker dependency and manual workarounds

The exercise underscored material operational dependencies on brokers, with direct effects on claims, renewals, and data exchange. Several agents observed that while crisis plans cover material third-party IT vendors, they do not always address distribution-led outages. Although workarounds exist (direct settlements, face-to-face trading, paper artefacts), many firms noted limited capacity to scale for extended periods or multi-broker outages, alongside challenges reconciling manual activity. In addition, some processes remain overly broker-centric for certain IBS, particularly FNOL, where policyholders may be unable to notify the managing agent because the broker is disrupted. Other examples included difficulty tracing exposure data and reliance on brokers to initiate in-person "claims surgeries" for urgent payments. Suggested next steps included formalising broker operational playbooks to document manual workarounds and recovery steps that prioritise process continuity (e.g., acceptable policyholder contact mechanisms for FNOL) rather than focusing solely on technology recovery; ensuring policy documents and websites provide explicit carrier contact options when brokers are unavailable; validating mailboxes, scripts, and triage flows; briefing frontline teams on FNOL pathways for third-party outages; joint third party testing; updating risk registers to reflect broker vulnerabilities; creating fast-path reporting to flag time-sensitive items within hours of disruption; and tracking time-to-contact and tolerance adherence through targeted exercises.

Disconnection/ reconnection protocols

Agents identified gaps in formal playbooks for disconnection and reconnection, including lack of clear criteria and approvals required before disconnecting, clarity on assurance artefacts needed for reconnection (e.g., independent forensics or internal risk assurance), designated authorisers, and rollback plans. In some cases, written protocols existed for IT vendors but not for distribution partners; in many cases, the documented protocols had not been tested, and practical constraints such as limited visibility of system-integration and data-flow dependencies would hinder efficient execution. Suggested next steps included increasing the granularity of resource mappings by creating end-to-end critical third-party dependency maps (IBS → process → critical third party → system/integration) with data-flow visibility; and creating and testing disconnection/reconnection playbooks for each material relationship, with clear decision rights, required evidence, phased reconnection steps, and dual approvals embedded into Crisis Response and IBS owner procedures.

Secure out-of-band communications & instruction verification

When normal channels were unavailable, agents reported limited secure alternatives and unclear identity-verification standards for urgent instructions, especially lead approvals. Several lacked senior, role-based broker contact hierarchies and pre-agreed verification methods. Examples included uncertainty over what constitutes sufficient proof in the absence of ECF/CLASS artefacts and limited access to vetted out-of-band platforms. Suggested next steps included formalising secure crisis-communication channels with critical third parties; defining pre-agreed alternative contacts with distribution partners; and setting evidence standards for lead agreement (e.g., system-artefact reference, wet stamp, attested PDF) published as a concise one-page aide-memoire.

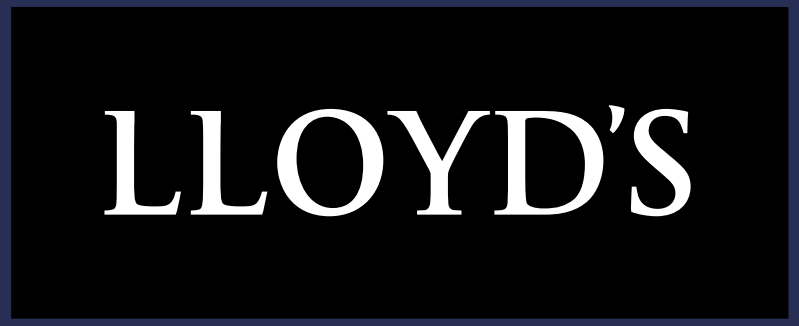
Market-level coordination & playbook standardisation

Consistent with previous tests, participants leaned on Lloyd's/LMCTG, Velonetic, and the LMA for coordination, assurance, and reconnection guidance, and many advocated market-wide standards to reduce duplication and accelerate decisions including refreshed Urgent Settlement Guidelines (USG) and a centralised approach to verifying claims agreements during platform outages. Suggested next steps included continued engagement and feedback loops with Lloyd's, LMA, and LIIBA to refresh USG and expand it to broker-outage scenarios; defining common verification standards; clarifying reconnection expectations with Velonetic; participating in joint exercises; and sharing learning artefacts (templates and aide-memoires) to raise the market's collective baseline.

2025 Market Wide Scenario Exercise

Thank you to all the participants that attended the Lloyd's 2025 Market Wide Scenario Exercise. We trust that the exercise has reinforced the importance of collaboration, preparedness and robust contingency planning to maintain operational resilience during unexpected disruptions.

If you'd like to contribute to the planning of the Lloyd's 2026 Market Wide Scenario, please contact us at MGRR@lloyds.com


LLOYD'S