[Covering the handover doc, GHD-ER-01 - Emergency Response Recommendations as promised in GovAlpha's notice of offboarding.]

GovAlpha Emergency Response Recommendations

TL;DR - Top Five Recommendations

- Implement an anon-friendly delegate notification process
- Pre-deploy flexible executive spells that can trigger Moms as appropriate
- Consider retaining former members of the Protocol Engineering Core Unit to assist in emergency response.
- Expand on the number of GSM exceptions
- Run regular delegate response drills

Emergency Response Overview

For a given emergency involving MakerDAO, there are four distinct stages that have the potential to limit emergency response time. These are:

- Detection
- Discovering the existence and nature of the emergency one needs to respond to.
- Coordination
- Deciding appropriate response to the emergency, and organizing contributing personnel.
- Technical Response
- Technical work required to respond to the emergency.
- Governance Response
- Mobilising MakerDAO governance to both understand and approve a given response.

Further, there is a fifth stage that doesn't limit response time, but that is also critical.

- Communication
- Explaining (to the extent it is wise and possible) what is happening, what is being done, and how stakeholders should respond.

Note that many of these stages can and should be performed in parallel, as often time-to-response is limited by the longest of these stages.

Detection

There are three main avenues that lead to the detection of an emergency.

Community Detection

In previous emergencies across the crypto space, issues have been detected by community members prior to detection by a compensated agent of the given DAO. Due to the global nature and level of community involvement in most DAOs, this is not surprising.

In Maker's case, this might look like messages in the discord about strange behavior in the protocol, or requests to speak to a compensated agent to disclose a presumed exploit. Often, these can be false alarms.

Maker's community is much less active at the current time than it has been in the past, and is much less active than some other DAO communities.

Automated Detection

Due to the accessibility and transparency of the blockchain, automatic detection of some emergency scenarios is possible.

In Maker's case, this would look like notification of key stakeholders by a number of agents within the DAO running

automated detection software. Most likely TechOps, Oracles, or Technical ecosystem actors.

It is not transparent exactly who is running what sort of automated detection software within MakerDAO. Nor is it clear whether it is tested and maintained regularly.

Developer Networks

Technical Ecosystem Actors, like most other types of ecosystem actors, maintain professional networks within the crypto space. This will often include both technical actors working at other protocols, and more security-focused actors like whitehats and audit firms.

In cases where issues in other protocols impact Maker, these networks are invaluable. Maker has frequently taken advantage of these networks in the past, for example with the CRVV1ETHSTETH-A oracle issue. Most notably, the contacts maintained by the members of the now-offboarded Protocol Engineering Core Unit.

Coordination

Coordination of emergency response in Maker has been an informal affair in the past. The coordination role tended to fall to one of the first individuals to respond to the emergency, who did not have an otherwise critical role. It was fairly common for the coordinator role to change hands as more people were brought in, in order to free up the previous coordinator to perform a role they were better suited for. In cases of extended emergency response, roles might change hands as people in different time zones come online.

While the Protocol Engineering Core Unit was active within Maker, they would often lead the decision-making as to what sort of response was required, discussing courses of action, seeking feedback from other stakeholders when they felt it was required and ultimately making a decision on the type of response to propose to MakerDAO governance.

Governance Facilitators have contributed in the coordination role in past emergencies, though it can be preferable to hand it off such that they can notify and contact delegates and large MKR holders without distractions.

The coordination role often makes a decision on which other stakeholders to bring into the response group, and when. This usually first involves discussion with currently present stakeholders as to the appropriateness of this action given any concerns around potential damage as a result of irresponsible disclosure.

Technical Response

The technical response stage covers the time between when an appropriate response is decided, and when that response is made available for approval by governance.

This stage is heavily dependent on two main factors:

- Emergency Preparation
- What responses have been created in advance to cover this emergency scenario?
- Technical Skill and Bandwidth
- How much capacity do the technical Ecosystem Actors have to produce a bespoke response?

Maker has a moderate level of preparation for a number of the most common issues in the form of exceptions to the GSM timelock delay. These exceptions are listed here. Further work could be done to expand the scope of these exceptions to cover more possible scenarios.

The technical skill and bandwidth available to MakerDAO for bespoke emergency response took a large blow with the departure of the Protocol Engineering Core Unit.

Governance Response

The governance response stage covers the time between a response or mitigation being ready to vote on, and being approved by governance.

The key factor in the time of governance response is the availability of critical delegates and MKR holders to vote on an arbitrary executive at any given time of day. Critical in this sense refers to the delegates or holders that are part of the minimum set of voters that are required to approve a response. Membership of this set varies due to the amount of MKR on the current hat proposal, and the relative MKR weights controlled by known delegates.

Previously, GovAlpha had sought and been provided with personal contact information for the larger Recognized Delegates. However, due to the new delegate structure requiring anonymity, this is no longer possible.

GovAlpha’s departure from Maker has the potential to further impact governance response due to the high trust with which it

is regarded, and due to a number of relationships developed over time between GovAlpha and key stakeholders.

Communication

As discussed above, communication is not a critical component of emergency response in the broad sense.

However, communicating well and swiftly can serve to limit both financial and reputational damage to MakerDAO and its stakeholders in the event of an emergency, and so should be taken extremely seriously. Clear communication can also prevent members of the response team from having to repeatedly answer questions about the situation in public discussion forums while giving people confidence that the issue is being handled.

In my opinion, Maker has not done well communicating during emergency response scenarios due to the lack of a professional and well-prepared communication team.

Recommendations

Implement an Anon-friendly Delegate Notification Process

Stage: Governance Response

The inability to reliably contact the Aligned Delegates could be a major blocker in an emergency response situation, depending on timing and severity.

0xDefensor shared a possible setup to resolve this issue in his postthere. We recommend such a process be implemented as soon as possible.

Pre-deploy flexible executive spells that can trigger GSM exceptional functionality

Stage: Technical Response

We have previously discussed this possibility in a forum postthere. To summarise, executives should be pre-deployed that are able to trigger the various GSM exceptions.

This would allow delegates to make some sort of response even in the absence of any technical stakeholder. It would also reduce the time-to-response for some of the most likely emergencies, even if the technical stakeholders are present and working on a more effective or appropriate response.

We recommend executive spells be pre-deployed for some of the most useful and widely applicable gsm exceptional functionality, as determined by technical stakeholders.

Consider retaining former members of the Protocol Engineering Core Unit to assist in emergency response

Stages: Detection and Technical Response

Former members of the Protocol Engineering Core Unit have proved to have useful industry connections, improving response time at the detection stage. They also have a large amount of domain knowledge of Maker and experience in dealing with previous emergencies.

GovAlpha recommends reaching out to some of the successor organizations with members from that unit and enquiring as to their willingness to act in an emergency response role only. ** **

Expand on the number of GSM Exceptions as appropriate

Stages: Technical Response

The GSM exceptions give Maker a fighting chance to react to an emergency situation early enough to mitigate protocol-ending damage. While the existing exceptions cover many of the most common scenarios, the exceptions should be expanded alongside the increase and change in Maker protocol functionality.

We recommend MakerDAO consider adding exceptions to cover:

- PSM liquidation.
- Debt ceiling freeze for more of the existing vaults using the LineMom contract.
- Universal Debt ceiling freeze, preventing any new DAI from being minted.

Technical Ecosystem Actors should be consulted to help identify any further exceptions that should be added.

Run delegate response drills

Stage: Governance Response

Irregular delegate response drills should be run by Scope Facilitators (likely the Governance Facilitators) in order to empirically measure likely delegate response times in various emergency scenarios.

We recommend that these drills take place four times a year, spread irregularly over the period.

Response statistics should be measured and recorded by relevant facilitators, or their agents, such that baseline response time and improvement can be tracked effectively. Statistics should be posted publicly unless clear harm will come from doing so.

Just having the drills will likely increase delegate response time, due to the reputational incentive of failing to respond quickly in drills. Regular drills should also help to highlight relevant issues in the emergency response process.

The last time this was attempted it received quite a bit of negative feedback from the delegates, it is worthwhile to consider making participation in drills a part of the delegate requirements in order to ensure that everyone is aligned.

Disclose the nature and status of automated detection mechanisms

Stage: Detection

Any stakeholders running automated detection software should regularly disclose what that software does, and deliver periodic public reports on uptime and test results.

This will help to highlight any clear gaps in automated detection and should encourage ecosystem actors to improve the reliability of these detection methods.

Technical Ecosystem Actors should actively develop social networks with other developers in the crypto space

Stage: Detection

Technical Ecosystem Actors working on the Maker Protocol should seek to network and improve their relationships with other developers, whitehats, and security experts in the crypto space.

We recommend MakerDAO fund this networking goal due to the clearly observed utility that these networks have provided in past emergencies.

Run Internal Emergency Response Drills

Stage: Coordination

Ecosystem Actors working on MakerDAO should run internal drills (ie with other Ecosystem Actors at Maker, but not involving governance) to practice, improve response and forge working patterns that can be relied upon in a true emergency.

We recommend that relevant scope facilitators organize these drills, observe, and provide feedback to the involved ecosystem actors.

Create an explicit emergency response framework

Stage: Coordination

In the past, the coordination stage has taken place largely informally, as mentioned earlier. While informality does allow for flexibility and the avoidance of bureaucracy at a time when it can least be afforded, it does have downsides.

An explicit emergency response framework could be descriptive rather than prescriptive. It could be assigned as required reading for relevant ecosystem actors and could include the following:

- The name and description of common roles, to ensure shared terminology and to reduce the likelihood of misunderstandings in an emergency.
- Description of commonly used communication and decision-making frameworks.
- A directory of the most-relevant stakeholders to contact in the event of various types of emergencies.

GovAlpha recommends the creation of such a lightweight response framework, alongside mechanisms to ensure relevant ecosystem actors become familiar with the contents.

Encourage meaningful community engagement

Stage: Detection

MakerDAO is currently not particularly welcoming or easy to engage with for potential community members for a number of reasons.

We recommend that this be worked on, in a general sense, in part due to the extra layer of reliability it can provide in the detection of emergency issues.