Major Incident Management

BACKGROUND

We all know that the standard Incident Management processes and procedures are not appropriate when it comes to managing a 'Major Incident'. The business and senior IT stakeholders will want an accelerated resolution and to be kept informed with progress. Making sure everyone knows what to do in the event of a Major Incident means having a well-defined process, strong leadership and clear communications.

At iCore we are constantly tracking what is happening in the IT World and particularly how that impacts IT Service Management. In doing this research we have noticed that in many cases a refresher on basic good practice is all that is required. To help our customers with this we have developed a series 'Back to Basics' guides on various topics (for a full list of related articles and guidance click here).

This IT Service Management 'Back to Basics' guide covers the essential considerations to deploy or improve MIM. It has been produced by Simon Hartley, Service Management Consultant at iCore, who has worked within major private and public sector organisations to improve the restoration of critical services.

GOOD PRACTICE REMINDERS

Have a strong Major Incident Management Procedure

Major Incidents are called such due to their impact on the Business and the additional demands that they place on the IT service delivery organisation. As such, a special procedure for handling them is required to:

- Accelerate resolution for incidents with high business impact which cannot wait to be resolved by standard Incident Management procedures.
- Provide accurate and timely communication to the impacted users and the management.

When you create or improve your Major Incident Procedure, you need to consider the following:

- When to invoke the procedure.
- How to build an effective Major Incident Team.
- How to manage the communications will be managed and the content for those communications.

Know when to invoke a Major incident

The decision-making to invoke the procedure must be straightforward with criteria agreed in advance and clearly documented. These criteria will focus on business impact but not all

'Severity 1' incidents require the Major Incident procedure – recurring incidents with well-rehearsed and rapid workarounds may not benefit from the additional MIM governance.

There are two approaches to the decision to invoke:

- Formal Criteria - State specifically when the procedure should be used, and when it should not be used.
- Guidance and Judgement - Have criteria as a guide for your Service Desk. Specify when they absolutely must use it, but leave it to their Business knowledge and judgment in less obvious cases.

The right team, with the right skillset, right mandate and right facilities

The right team will depend on the scale of the services being provided and the impact and complexity of the incident - clarity about roles and responsibilities is essential.

The following roles are essential:

- **Major Incident Manager:** Directs the resolution effort; brings resolver groups together into a coherent and effective team; secures additional resources where necessary; faces off to senior Business stakeholders; resolves any conflicts of interest (such as impacts on projects).

  The Major Incident Manager has to be sufficiently senior to achieve the tasks outlined above whilst also having the necessary familiarity with the technical aspects to build and execute a coherent recovery plan. For this reason, the Major Incident Manager may not be a permanent appointee and may be selected from a pre-agreed list depending on the focus of each Major Incident for example a Service Manager or Head of Applications Management.

  One thing that has to be clear is that the Major Incident Manager is king in the Major incident Management Room. If they save write this down then write it down; if they say get out my room, then get out the room (even if you are the CIO!)

- **Major Incident Co-ordinator:** Supports the Major Incident Manager by coordinating communication with resolvers and the Business. The co-ordinator sets up conference calls; captures and follows-up resulting actions; drafts, gains approval for then issues communications; manages the incident clock for both escalation and task progress.

  The co-ordinator may often be provided from the Incident Management Team and should be supported by that team where necessary.

- **Resolver Group Representatives:** Goes without saying… required to investigate the incident and affect a resolution. These can be internal groups or third parties.

The Major Incident Team should also include:

- **Problem Manager:** To capture information arising from service restoration that will aid subsequent root cause analysis (this activity must not compromise the restoration of the service).
- **Technical Architect or Project Resources:** To provide additional subject matter expertise where required.
- **Vendor Representatives:** Where third-party supported services are involved.

- **Business Representatives:** Business Relationship Managers or similar who can represent the Business interests; arrange and provide feedback on user testing; to help secure permission for the impacting of other services required to progress the resolution.

The Major Incident Management Room is a room that is assigned to be commandeered by the Major Incident Team in the event of a Major Incident, regardless of it being used at the time or not. The room should be kitted out with the necessary kit and facilities to manage the major incident, including conference facilities, whiteboards, and the Major incident process documented with roles, rotas, and even tea and coffee making if appropriate.

Excellent Communications

Much of the value of a MIM procedure comes from improved communication above and beyond that from the regular Incident Management Process. For this to be achieved, a pre-agreed Communication Plan, templates and well trained staff are all essential.

Separate the communications to Business, Senior Management and Resolver Groups

- For Resolvers Groups, the Major Incident teleconference is the main communication tool. A strong MIM team on a teleconference and WebEx can coordinate the efforts of multiple resolver teams, enable salient questions to be posed and answered, remove misunderstanding, minimise handover delays and enable parallel activities. This will reduce time to recover compared with a serial/silo'd/ping-pong approach.
- For the Business, frequent, concise communication in language that end users can understand will limit frustration and provide the Major Incident Manager and resolvers with the necessary breathing space to focus on Major Incident resolution.

To ensure that Business communications are as effective as they can be, you should agree in advance the media to be used the frequency, level of detail and standard templates that will drive the desired level of quality. The following list of media all have their uses and should be considered based on the Business need:

- Conference Call – The resolver teleconference will have detail that Business people don't want or need, having Business representatives on this call risks 'airing dirty linen in public'. Consider a separate call for the Business, attendees of should be responsible for cascading the messages to their Business areas.
- Email messages – Template-based, with pre-agreed distribution lists (Global or targeted based on the scope of the impact). These are a one-way communication so the language has got to be right. A good idea is to have all these emails QA'd and approved before issuing.
- Text message – Good for keeping key stakeholders up to date, particularly out-of-hours, particularly when a recovery plan is proceeding as agreed. A template to ensure brevity and clarity are essential when using SMS.
- Service Desk Telephony – Regular updates on the IVR system can keep end-users up to date and prevent the fielding of unnecessary that don't add to the investigation and resolution. (e.g. "Press 1 to hear an update on all MIs affecting service").
- Intranet – A Service Status Page, updated regularly with affected business areas, business impact and expected time to recover can be effective if you can educate

users to visit. Consider a traffic light indicator on the home page to warn of outages which links to the service status page. Such an arrangement can be used for scheduled outages due to changes also.

Getting the communication right is difficult BUT the rewards are great, so you should actively seek feedback from users: are the messages useful? Was the language understood? Was the Business impact accurately described? Do they want more communication or less? Does one size fit all?

Listen and improve, it will be noticed and appreciated.

Major Incident Review (MIR)

A Major Incident will be, by definition, a stressful event so it is essential to make the most of the opportunity to learn lessons to minimise the risk or impact of a recurrence to improve the Major Incident procedure itself. A Major Incident Review will summarise the resolution history, capture any perceived root causes and provide a key input to the Problem Management process, and identify opportunities for procedural and service improvements.

A well-conducted Major incident Review can also help the IT organisation restore confidence potentially lost during the incident itself.

If you are looking for someone to help you get your Major Incident Management process into a good place, or want someone to come in and lead by example, then give iCore a call.

Contact us on +44 (0) 207 464 8414 and info@icore-ltd.com

service management at its best