Major Incident Masterclass

Vawns Murphy

@vawns / @ITSM_tools / @wearesilvahomes

vawns.murphy@gmail.com

uk.linkedin.com/vawns

Introduction

- Worked in ITSM for almost 20 years
- Regular speaker at industry events
- Worked in all sorts of organisations, large and small
- When not child wrangling or being pelted with brightly coloured balls in the name of ITIL, is the Lead Partner for IT Service Delivery at Silva Homes.
- Finds her job quite fun

Agenda

- What is a Major Incident?
- First things first
- Sanity check
- Communication
- Action Plan
- Updates
- Fix
- Closing the loop
- What can we do better next time?

Image Credit: 123rf.com

What Is A Major Incident?

- ITIL definition: The highest category of impact for an incident. A major incident results in significant disruption to the business.
- In other words – the serious stuff.
- Real life examples; email outages, cyber attacks, service downtime
- In short – anything that causes this reaction.

Image Credit: teespring.com

First Things First

- Take a moment to understand the impact
- Remain calm
- Don’t cause panic
- How I do all of the above:

Sanity Check

- Are your people ok?
- The service affected and business impacted.
- The support team involved
- Is there a workaround
- Do we know how long it will take to fix?
- Do we need to invoke DR?

Communication

- You need to tell right people at the right time with the correct level of information.
- Ideal world: everyone is made aware as soon as reasonably possible.
- In reality? IT, senior management then the business.
- What to include:
- Incident overview and reference number
- Affected service
- Any workarounds
- Time of next update

Action Plan

- Gather your team players
- Recap the facts
- Ask for solutions
- Check if more support is needed
- Keep things on track
- Be prepared for things to get tense and know how to manage people if things get fraught

Updates

- Commit to a comms schedule
- Meet deadlines
- Tailor your updates to your audience

Fix

- Check it works and then check it again
- Have another person to sanity check if possible
- Deal in change management
- Trust but verify – how do we know it’s worked?
- Closure comms

Closing The Loop

- Capture key actions
- How was it fixed?
- What can we do better next time?
- Do we understand the root cause?
- Loop in Problem Management
- Engage BRM & SLM
- How do we prevent recurrence?

Key Takeaways & thank you

1. **Major Incidents are more serious than your typical faults**

   - they are show stoppers and need to be treated as such

2. **Keep calm**

   - you can't help anyone if you start to panic

3. **Get your facts straight**

   - so you know what you're dealing with

4. **Gather your A-Team**

   - to agree an action plan & manage comms

5. **Just fixing it isn't good enough**

   - you need to understand the root cause and identify any further preventative actions