Some aspects of Software Applications for Incident Analysis

Colesnicova Vlada, Academia de Studii Economice din Moldova, Chișinău, colesnicova.vlada@ase.md
Conducător științific: **dr. Tutunaru Sergiu**, Incubatorul Inovațional IT4BA, Academia de Studii Economice din Moldova, Chișinău,tutunaru@ase.md

Abstract: Incident management can improve the quality of IT services by identifying the recurring incidents and logging problem tickets to identify the root cause of the incident/ incidents. If there is any recent incident with no resolution, then a problem ticket is created to identify the root cause and fix it. By identifying the recurring incidents and their associated CI's, availability management or capacity management or information security management, or continuity management can redefine or revise the respective plans and procedures to improve the delivery of services.
Goal: The prime goal of incident management is to resolve incidents either with temp fix or perm fix and bring back the IT service. Resolving the incidents firstly requires registering the incident in the ITSM tool with a unique reference number. Categorization of the incident is done based on hardware, software, etc., and then the incident is assigned to the appropriate team or a person to take quick action. The investigation and diagnosis are made. The resolution is implemented by searching knowledge articles or reference materials or KEDB, and once the issue is resolved, the incident is closed.
Design / methodology / approach: This process is focused on returning the performance of your organization's services to normal as quickly as possible. Ideally, in a way that has little to no negative impact on your core business. This means incidents sometimes rely on temporary workarounds, while you identify the root problem of an incident afterwards.
Finding: No modern system would be truly keeping up with technology if it did not utilize machine learning and AI to continuously improve upon itself, and IMS is no exception.
Limitations / implications of the research: Even though "incidents" may have a negative tone, they do not have to interrupt or shut down your operations. By implementing an incident management system, you empower your enterprise to prepare for the inevitable incidents that will come — and ensure the team can swiftly and effectively remedy any situation.
Practical implications: Help desk and incident management teams rely on a mix of tools to resolve incidents, including monitoring tools to gather operations data, root cause analysis systems, incident

management and automation platforms, and other support products.

The value:

- **Guide and build**: Incorporate autonomous decision-making and consistence culture among teams in identifying, managing and learning from incidents. There will not always be a clear answer, but guiding and building together can move the process along more effectively.
- **Align teams**: Develop an understanding of which attitude is appropriate for each aspect of incident identification, resolution and reflection.
- **Detect**: Continuously monitor and attend to incidents before customers discover them, as issues can be resolved before becoming incidents.
- **Respond**: "Don't hesitate to escalate." It is better to bring awareness of a potential incident even if it does not affect everyone than to stay silent.
- **Recover**: Service will go down time to time uncontrollably; this is understood as long as the incident is resolved as quickly and efficiently as possible.
- **Learn**: In reference to the value above, mistakes or accidents will occur but proper accountability and gained knowledge from those situations can improve for better delivery of service.
- **Improve**: Break down the incident, starting from the exact root cause to the necessary and strategic actions in preventing or reducing the chance of the incident occurring again. Set dates for those actions.

Introduction

IT incident - what is it in simple words?

An IT incident is a technical disruption to a workflow or, in simple terms, an event that is not part of the normal operation of an IT infrastructure. A technical incident can be any incident that has an impact on hardware and software. For example, lack of free space on the hard drive of a work laptop and data leakage with the disclosure of confidential information are IT incidents, but with varying degrees of significance for the enterprise. Incident management strategy (ITSM - IT Service Management, IT service management) is called upon to correct the situation and return everything to normal.

Examples of incidents in the IT field

- Unauthorized access, use, disclosure, modification or destruction of information.
- Interference with information technology (intentional or accidental).
- Violation of policies, laws or regulations relating to IT infrastructure.
- Failure of equipment and software due to various circumstances (force majeure or predictable).
- Identification of deviations and shortcomings in the functionality of hardware and software.

Defining, Prioritizing and Classifying an Incident

An IT incident is typically defined as an unplanned interruption or reduction in the quality of an IT service. Although prioritization of incidents can vary from organization to organization, incident priority is typically determined by two factors:

1. Impact, or degree of failure, and how many end users does the incident affect.

2. Urgency, or the importance of the services affected, relative to the mission of the organization.

Impact and urgency are also influenced by many different factors including:

- Customer or business need
- Financial impact
- Service criticality
- Business risk

- Component failure impact analysis
- Legal requirements
- Et cetera.

Incidents are also typically divided into two buckets:

- Normal Incidents: A scenario in which we have a disruption in context of a service definition such as a SLA. Most, but not all, impact users. Some normal incidents, such as failures that trigger redundancies, do not impact users directly but should be resolved before they do.
- Resolvers work through normal incident management in linear steps: logging, categorization, prioritization, initial diagnosis, escalation, investigation and diagnosis, resolution and recovery, and closure.
- Major Incidents: Incidents have a large, impactful effect on the organization, or have time constraints are defined as major incidents. Working through major incidents involves case management workflows as opposed to linear steps, meaning hypothesis testing and probing through experimentation.

Systems should be categorized by importance and have SLAs around how long they can be unavailable before escalation. Impact and urgency will determine if normal incident or major incident processes are followed, and when SLAs exceeded, the organization has run out of time for experimentation and must move onto the IT service continuity / disaster recovery plan.

Incident Management Roles and Responsibilities

Because the different levels of incident management trigger different processes for response, it is critical to define roles and responsibilities for execution. These roles and responsibilities define who will drive process improvement, report key performance indicators (KPIs), and execute and enforce process workflow. They also define lines of communication between the IT team, the rest of the organization, vendors, and third parties.

Improving IT Incident Management

Minimizing the effects of service interruptions has a direct effect on a business's bottom line. The cost of downtime in businesses can be astronomical. According to Everbridge's State of IT Incident Management Report, the average cost per minute of an unplanned downtime is $8,662 US, which represents more than half a million dollars per hour. In the event of an IT incident, our research has shown that it takes IT organizations an average of 27 minutes, maxing out at 150 minutes in some cases, to assemble the response team. By automating this process, organizations are able to engage the response team in 5 minutes or less, minimizing the negative impacts of an incident and reducing the overall incident management timespan. In the midst of a crisis, there is no time to hunt for the right people or write the message language. IT Service Alerting tools, as defined by Gartner, can reduce "mean time to respond" by automating the manual process typically associated with the response process.

Support staff responsible for managing a critical incident should have the ability to:

- Contact the appropriate teams for any given incident
- Contact those who are on call without hunting for the information
- Immediately start a technical conference bridge with the right people
- Inform the stakeholders and business management
- Notify key customers and impacted users
- Send messaging that is compliant with HIPAA and other regulations
- Apply remedial actions according to predetermined, automated workflows

What are the benefits?

In short, the benefits of Call Management include:

- Improved efficiency and productivity. Your service desk agents use the same process for

handling each incident. This takes away any guesswork.

- More visibility and transparency. By handling incidents according to this process, callers know what's happening to their tickets and when.
- Higher level of service quality. Your agents won't lose track of tickets in a mailbox or pile of post-its again. Agents can also easily prioritize tickets, so the most critical incidents are picked up first. This gives your organization's callers more certainty about the continuity of your (IT) services.
- More insight into service quality. You actively register all incidents in your Incident Management software. As a result, your organization gains valuable insights via monitoring and reporting. For instance, which type of printer gives your callers the most trouble? Or which type of incidents repeatedly aren't resolved on time?
- Meeting SLAs. The Ticketing Management process gives you more insight into your SLAs. And whether you're meeting them. This gives you the opportunity to take action where needed.

Conclusion

In a perfect world, everything would run smoothly, and there would be no such occurrence of incidents. However, the real world has proven endless times that it hides nothing from the possibility of problems happening now and then. With that said, it is important to identify the cause of incidents, develop consistent procedure to resolve among dedicated teams, plan actions that can reduce or prevent re-occurrence, and learn from each one to tackle those situations accordingly.