



Incident Response Plan

2023-08 @Guzhongren

Agenda

- Definition of Incident
- Incident Severity
- Pre-Actions for the Incident
- Incident Response
- Post Actions of the Incident
- Q&A

Definition of Incident

What

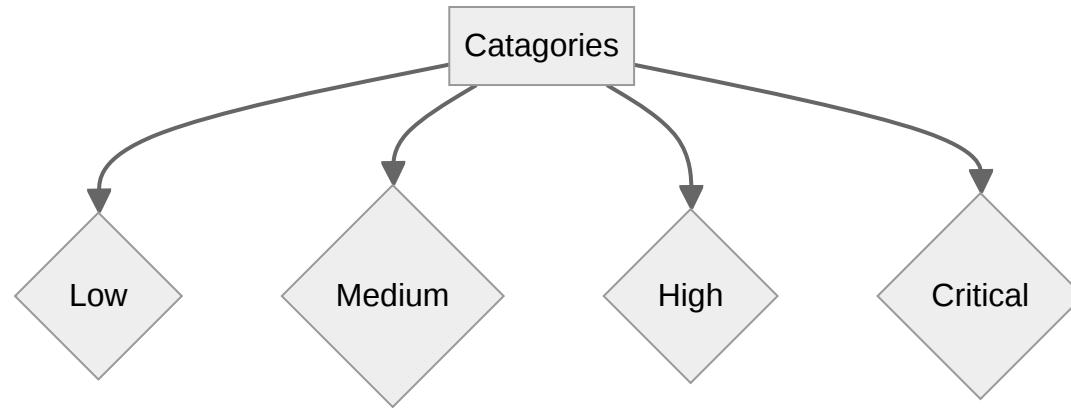
An incident is any **real or suspected event** that affects the **confidentiality, availability or integrity** of the **company or any client's information or systems.**



Incident Severity

Incident Severity

Catagories



| Severity | Characteristics | Response Time | Status Reporting | Target Resolution/Bypass time | Examples |
|----------|--|---------------|------------------|-------------------------------|---|
| Critical | <ul style="list-style-type: none"> * Requires executive level attention * Affects business globally * Poses a significant and immediate threat to human safety * Has a high probability of affecting or spreading to client systems, data centers or affecting public, customer or third-party systems | Within 1 hour | Every 1 hour | Within n hours | <ul style="list-style-type: none"> * Breach that involves secret, private or sensitive client information * Irrecoverable loss of business critical data (billing, accounts receivable) * DoS attack on public facing sites * Attacker is able to publish information acting as the client |
| High | <ul style="list-style-type: none"> * Requires attention of CIO and/or regional business leadership * Affects the ability of entire regions or teams from doing their work * Poses a significant financial, legal, commercial or reputation's risk to company * Has a high probability of affecting or spreading to other systems | Within 2 hour | Every 2 hour | Within 2n hours | <ul style="list-style-type: none"> * Unauthorized access to confidential, private or secret information * Recoverable loss or corruption of critical data * Critical security patches not applied |
| Medium | <ul style="list-style-type: none"> * Requires InfoSec and Legal team attention * Limited to a single or small group of locations * Poses a moderate financial, legal, commercial or reputation's risk to company and/or our client * Has a moderate probability of propagation to other systems or networks | Within 2 days | Every 2 days | End of the issue solved | <ul style="list-style-type: none"> * Unauthorized access to internal information or systems * Recoverable corruption or loss of isolated non-critical data * Disrupts our ability to work on more than one project. |
| Low | <ul style="list-style-type: none"> * Characterized by impacting a single or few non-critical systems * Affects a single user or a small number of people * Has no or very low probability of propagation to other systems or networks * Has little or no effect on business operation; likely can be handled via BAU | Within n days | Every n days | End of the issue solved | <ul style="list-style-type: none"> * Loss or theft of mobile devices and laptops * Phishing * Lost access card * Unpatched libraries with low vulnerability scores * Credential leakage to private repository * Sensitive information leakage to internal Logging solution * Near misses |

Pre-Actions for the Incident

Pre-Actions for the Incident

Contact List

| Role | Name | Primary Location | Phone Number | Email |
|---------|----------|------------------|--------------|--|
| Someone | TL | 2F | 12345678 | incident@incident.com |
| Ops | Ops team | China | 1234556 | ops@incident.com |

Pre-Actions for the Incident

Domain Owner

Domain

Biz Owner

Tech Owner

Payment

Eric

John

...

...

...

Pre-Actions for the Incident

Stakeholders

| Role | Name | Email | Biz/Tech Responsibilities |
|------|-------|--------------------|---------------------------|
| PO | James | james@incident.com | xx biz owner |



Pre-Actions for the Incident

Rehearsal

- Take a recent incident to rehearsal with **the whole team members**
- Clarify everyone's **responsibilities**
- ...



Incident Response

Incident Response

YOU SHOULD

- **Keep cool and calm**
- **Determine the severity**
- **Do NOT destroy any evidence**
- **Try to standby with team/on-call host**
- ...



Incident Response

Medium

On-call host

- Collect necessary information
- Connect PM & TIs
- Analyze the potential root cause
- Monitor the online resources, products
- ...

PM/Ops Leader

- Report the progress of the incident
- Create an issue card on Jira/ServiceDesk
- ...

Incident Response

Medium

TLs

- Track/review the solution of the fixing
- Track the deployment
- ...

Domain owner

- Sort out the biz flow
- Code fix & Verify & Monitor
- Report the proress of the bug fixing
- Showcase
- ...

Others

- Keep an eye on the bug context

Incident Response

Critical

- SIRT(Security Incident Response Team) formed
- Requires executive level attention
- Emergency response
- Other requirements regarding incident response (e.g. from client side or compliance perspective) also should be taken into consideration.
- Requires senior leadership or MD review of incident report
- Triggers new Enterprise Risk Assessment and BCP review

Incident Response

High

- SIRT formed
- Immediate response
- Other requirements regarding incident response (e.g. from client side or compliance perspective) also should be taken * into consideration. Refer to Other References section
- Requires Legal / InfoSec review of incident report

Incident Response

Medium

- SIRT formed
- Routine response
- Other requirements regarding incident response (e.g. from client side or compliance perspective) also should be taken into consideration. Refer to Other References section
- Requires CST review of incident report

Post Actions of the Incident

Post Actions of the Incident

PIR(Post Incident Report)

| Item | Content | Note |
|--|---|------|
| Tracking ID | xxxx | |
| Type | Incident | |
| Impacted Services | xxx | |
| Impacted Regions | xxx | |
| What happened? | Current behaviors | |
| What went wrong and why? | Root cause | |
| How did we respond? | [Timeline of processing] Who... does what...when... | |
| How are we making incidents like this less likely or less impactful? | | |
| How can customers make incidents like this less impactful? | | |
| ... | ... | ... |

Post Actions of the Incident

Retro

- Go through the key point of the incident
 - Who... does what... when...
- Summary the executable actions for team
- Lesson and Learns

Q&A

Thank You!