OWASP

Open Web Application Security Project

Top 10 Considerations For Incident Response.

By: Tom Brennan, ProactiveRISK

Table of Contents.

1. **Introduction.**
2. **Consideration #1: Audit and Due Diligence.**
3. **Consideration #2: Create a Response Team.**
4. **Consideration #3: Create a Documented Incident Response Plan.**
5. **Consideration #4: Identify your Triggers and Indicators.**
6. **Consideration #5: Investigate the Problem.**

OWASP
Open Web Application
Security Project

Table of Contents.

7. Consideration #6: Triage and Mitigation.

8. Consideration #7: Recovery.

9. Consideration #8: Documentation and Reporting.

10. Consideration #9: Process Review.

11. Consideration #10: Practice , Practice , Practice.

12. Conclusion.

OWASP
Open Web Application Security Project

1.Introduction.

Open Web Application Security Project

A Security incident is an identified occurrence or weakness indicating a possible breach of security policies or failure of safeguards, or a previously unknown situation which may be security relevant.[1]

Incident Response is the reaction to an identified occurrence whereby responders classify an incident, investigate & contain the incident .

OWASP
Open Web Application
Security Project

Why is Incident Response Important?

The answer is straightforward. Any challenge or problem which is not properly contained and handled can and will spiral into bigger problems that can eventually lead to the total collapse of the system.

OWASP

Open Web Application Security Project

WHY IS INCIDENT RESPONSE IMPORTANT?

RESTORE SERVICES

MITIGATE WEAKNESSES

MINIMIZE LOSS

REDUCE RISK

One of the biggest questions that must be answered by companies or Incident Response Managers is:

“Where do we start from?”

Consideration #1: Audit and Due Diligence.

Performing an audit will let you know how well prepared the organization is for Incident Response in terms of:

PEOPLE

PROCESS

EQUIPMENT & MATERIALS.

OWASP
Open Web Application
Security Project

Consideration #2: Create a Response Team.

Preventing and managing attacks or incidents that can occur without prior notice is best managed by experts that belong to an Incident Response team.

Some important things to note when creating an Incident Response Team.

- Ensure that you have a competent Team Leader who is in charge and has a clear chain of command.
- Document the roles and responsibilities of the team members and communicate this clearly to all relevant stakeholders.

Open Web Application Security Project

Consideration #3: Create a Documented Incident Response Plan.

OWASP
Open Web Application
Security Project

An organization should have a well-documented Incident Response plan that would guide the Incident Response Team during an incident.

**A comprehensive plan at minimum , should cover Roles and Responsibilities,
Investigation, Triage and Mitigation, Recovery, and Documentation process.**

OWASP
Open Web Application
Security Project

Consideration #4: Identify your Triggers and Indicators.

What would be categorized as an incident at your organization? How important or weighty are the factors that would trigger an incident?

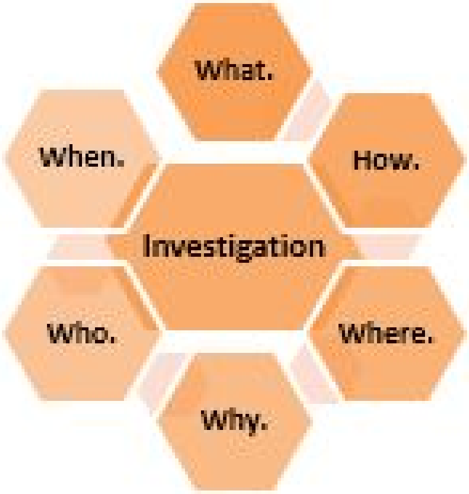
You need to clearly define what can trigger an incident. Some of these events include:

- Loss or theft of Equipment.
- Loss or theft of Information.
- Attempts to gain unauthorized access to data, computer or information storage device.

Consideration #5: Investigate the Problem.

A thorough investigation will require input from the Incident Response Team and might require input from external resources.

The investigation will document the incident details, including what to look for, who to involve, and how to document what is found.



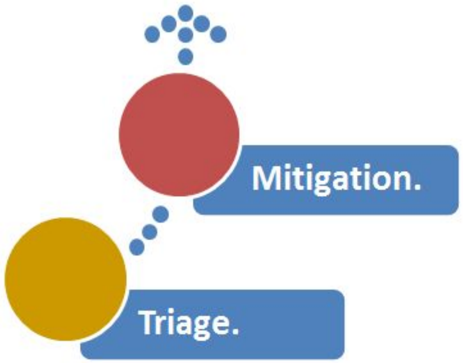
OWASP
Open Web Application
Security Project

Consideration #6: Triage and Mitigation.

Investigation leads to the triage & resolution process. As the team identifies potential exposure , they should plan & execute effective mitigation accordingly.

In summary , the triage process should cater for the following activities:

- Classification of the Incident.
- Incident Prioritization.
- Assigning specific tasks to specific people.



Consideration #7: Recovery.

Recovery is a significant step for restoring whatever services or materials might have been affected during an incident.

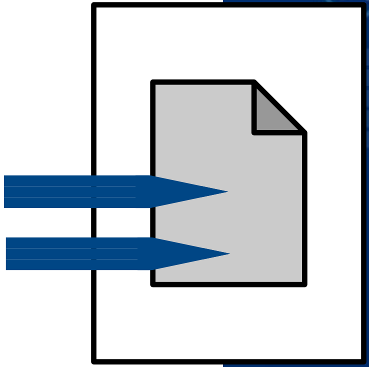
- **The recovery step is the transition from active incident to standard monitoring.**
- **The recovery procedure should include the steps for transition given the specifics of the firm’s environment and approach.**

OWASP
Open Web Application
Security Project

Consideration #8: Documentation and Reporting.

Reporting and documentation is a critical action that will always occur before, during and after Incident Response.

- A comprehensive incident report is required in keeping with best practices and with the Incident Response plan. The type of reports that might be required might vary but should help in managing and reviewing incidents satisfactorily.

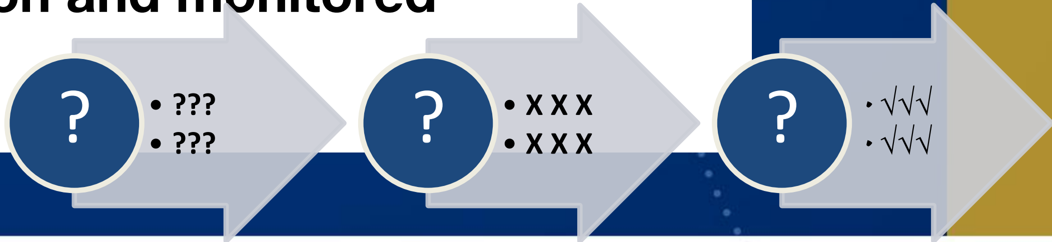


Consideration #9: Process Review.

It is imperative to continuously monitor an incident and the workload/performance of the team or Incident Handler.

Process Review can help you to answer the following:

- **Should I increase or decrease the number of Incident Handlers?**
- **Do we need to develop automated procedures for Incident Handling?**
- **What risks did we identify during the incident that needs to be followed up for action and monitored closely ?**



?
- ???
- ???

?
- X X X
- X X X

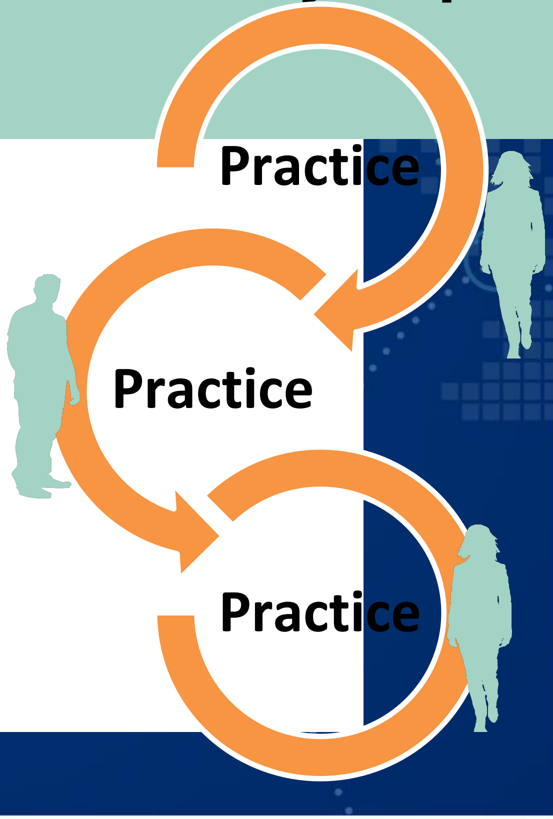
?
- √√√
- √√√

OWASP
Open Web Application
Security Project

Consideration #10: Practice, Practice, Practice.

Do not wait until an incident occurs before you put your team to work.

- It is important that you Incident Response Team understand how important mock drills and practice are to the firm.
- Sometimes you can practice the organization's plan by simulating a live scenario.
- This test can be as simple as dropping a thumb drive on the floor of the office and seeing what happens, to simulating a data breach or phishing attack.



OWASP

Open Web Application Security Project

Conclusion.

Incident Response cuts across the whole organization and should not just be restricted to the IT unit or particular units.

- **It should be clearly communicated that an organization's service delivery can be endangered when incidents occur.**
- **Incident Response Team has the mandate to prevent , handle, resolve and adequately document incidents that may arise.**
- **Incident Recovery is a significant tool of overall governance and to have it is a necessity. This fact is acknowledged and supported in the ISO 27001 security standards and in frameworks such as ITIL and COBIT.**

Questions?

Tom Brennan
tomb@proactiverisk.com