



OWASP

Open Web Application
Security Project

Top 10 Considerations For Incident Response

Project Leaders / Authors

Tom Brennan, ProactiveRISK

Jason Jolo, ProactiveRISK

Technical Reviewers

Jordan Lewis

Version 2.0

2-December-2015

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.
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.

1. Introduction

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]

Organizations are susceptible to different types of attacks which might be simple or sophisticated in nature and **attack vectors** such as attempted hacks, viruses, and trojans keep evolving at a pace that calls for constant vigilance. Incidents have the potential to affect the confidentiality, integrity and availability of information or services provided by an organization.

Incident Response is the reaction to an identified occurrence whereby responders classify an incident, investigate and contain the incident . Incident Documentation is also a part of this procedure which should be conducted in an efficient and timely fashion. More often than not, many companies fail to appreciate how much they stand to lose when they do not have the people, processes and tools that are required for **Incident Recovery** procedures. Statistics reveal that security incidents now occur on a regular basis and cause substantial business interruption when it is not well handled.

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.

Incidents will occur even in environments that are adequately prepared for it.

A competent **Incident Response** operation will help to

- Minimize loss.
- Mitigate the weaknesses that were exploited.
- Restore services and processes.
- Reduce the risk that can occur from future incidents.

WHY IS INCIDENT RESPONSE IMPORTANT?



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

“Where do we start from?”

Our advice is that you do a comprehensive **audit or review** of your constituency in order to have a very good picture of where the organization stands.

2. 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.** Is there a formal Incident Response team? if yes , do the team members have adequate technical skills for the designated roles or tasks ?
- **Process.** When an incident occurs do the team members know what to do, when to do it and how to do it?
- **Equipment and Materials.** Has the organization identified the equipment, materials or information mission critical to the business? Where are such equipment or materials stored? What are the interactions between business processes, supportive systems and external suppliers? Are these interactions monitored and documented ? etc. All these questions and more will be answered when an **audit** is performed.

Remember due diligence will expose the problems an organization can face in implementing an effective **Incident Response Plan**.

3. Consideration 2. Create a Response Team.

In an era where business and business interactions are conducted at a very swift and extraordinary pace, it is amazing to note that only a few organizations totally comprehend how ready they are to react to incidents that affect their organization.

Preventing and managing attacks or incidents that can occur without prior notice is best managed by experts that belong to an **Incident Response** team. Organizations or enterprises without an **Incident Response** team should know that it is **essential** to create an **Incident Response** team whose objective is to set priorities for managing, responding to and recovering from incidents.

An **Incident Response** team should consist of people with sufficient technical skills. It is important that the team members consist of SME's (Subject Matter Experts) or Knowledge Engineers from different domains across the organization.

The following roles are important to any IR team:

- **Team Lead.** The responsibility of the Team Lead is to coordinate the efforts of the team and ensure that assigned tasks are executed in an efficient manner.
- **Triage Officer.** The Triage Officer deals with incidents that are reported to or by the team. The resource person occupying this position will need to decide whether it is an incident that is to be handled by the team, when to handle it and who is going to be the incident handler according to laid down procedures.
- **Incident handler.** The incident handler role is important. The handler deals with the incident analyzing information, proposing solutions, resolving incidents and communicating progresses or challenges faced.

You might also consider Vendors and Third party Service Providers whose activities are relevant to **Incident Management**. They should help you to respond to incidents in a faster, more effective manner.

Other members of the team can be a Public Relations Officer, Legal Adviser and a Risk Assessment officer.

In summary there are 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. This will ensure that the work flows smoothly along clearly established reporting lines.
- Team members should have sufficient authority to respond to task and challenges within their jurisdiction. They should also be encouraged to work actively with other internal and external team members as the overall objective is to respond efficiently to **incidents** that affect the organization as a whole.

Remember, the major task of the **Incident Response** team is to classify an incident , investigate and contain the incident and also ensure proper documentation where applicable. A team is only as strong as it's weakest link. Ensure that all team members realize how important their roles are and review performances and contributions accordingly. Ideally you should have backups for these roles when the team members are unavailable.

4. Consideration 3. Create a Documented Incident Response Plan.

An organization should have a well-documented **Incident Response** plan that would guide the **Incident Response** Team during an incident. There are many sample documents available which can help you in this exercise. Any plan drawn up for the team and firm must be practicable and in accordance with best practice. A good starting point is to start off with standards such as the ISO/IEC 27000 series.

However, in a bid to follow best practice , do not draft a plan that will not be feasible for your team and organization . You can ask an auditor, a third party expert or an ISO 27001 certification body, to confirm that your incident response plan is at par with your standard practices.

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

These steps should be actionable by members of the **Incident Response** Team. Executives should be familiar with the plan and equipped with appropriate procedures for handling outside inquiries.

5. Consideration 4. Identify your Indicators and Triggers.

What would be categorized as an incident at your organization? How important or weighty are the factors that would trigger an incident? It is not every event that occurs that will trigger an incident or an incident response. This implies that 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.
- Unauthorized software or hardware installation.
- Unauthorized information transmission within the organization or to an external party.
- Attempts to gain unauthorized access to data, computer or information storage device.
- Unauthorized clearance of sensitive data or information.
- Attempts to compromise or breach defined security networks within the organization
- A member of your organization reports of suspicious activity such as clicking on a phishing link.
- A Web server's log entries that that indicates the use of a vulnerability scanner.
- A host's audit log indicating a suspicious change in its configuration. Just to mention a few

These **triggers** or indicators should be documented. It is advisable that it also goes into your documented Incident Response Plan (see the previous section for more details) and known to the all members of your organizations . This may require some training or a comprehensive awareness campaign as the information should not be limited to the **Incident Response** team.

6. Consideration 5. Investigate the Problem

When an event occurs, an **Incident Response** Team is required to categorize the event and identify whether or not you have an incident. The review will determine if it is a valid potential incident or not.

A thorough investigation will require input from the **Incident Response** Team and might require input from external resources (see Incident Response Team members above).

In investigation, the necessary course of action will depend on the cause of the incident and plan according to the Incident Response documentation. Note that some incidents can be fixed swiftly while some may take a while to resolve.

In any scenario, communication within and without the team is very important and all stakeholders should be briefed accordingly. The investigation will document the incident details, including what to look for, who to involve, and how to document what is found.

Some other activities that can be carried out are listed below.

- Establishing , clearly what has occurred.(Is it a malware attack, system hack, session hijack, Denial of Service etc)
- Identify what systems, people or processes have been compromised or affected based on incident.
- Determine what happened to what was compromised.
- Determine the point of origin of the incident where possible .This infers that you establish the source of the threat or attack vector.
- Specifying your investigation objectives, triage and resolution methodology.

- Gathering , reviewing and detailed analysis of all information concerning the incident,
- Adequate checks on equipment for malfunctions and vulnerability that may have led to the incident.
- What information (if any) has been disclosed to unauthorized parties, deleted or corrupted.
- Identifying the potential business impact of the incident: i.e. Business Interruption , Financial Loss.
- Other investigative procedures to be carried out like Forensics , Prosecution etc

For example , if the Incident has to do with a compromised equipment within a network, it will be advisable to determine which equipment was compromised, if the compromise came from an external or internal source. If it is determined that the incident merits probable legal action, preserving the evidence in its original form will be a crucial requirement. The Legal Counsel will recommend proper steps for documenting the evidence and collaborate with Law enforcement agencies where necessary.

7. Consideration 6. Triage and Mitigation.

Investigation naturally leads to the triage and resolution process. As the team identifies potential exposure, they should plan and execute effective mitigation accordingly. For various incidents, the plan should include the incident type and necessary steps for mitigation.

Some mitigation steps and actions have been listed in the previous section (see Investigation above).

For some incidents, the response may require more complicated and coordinated actions to remove the attack vectors or attackers from your environment. Some organizations may not have the expertise or experience to execute and document all steps and would require external input. The details for vendors who may need to respond, such as an ISP during a Denial of Service attack, or a forensics firm to mitigate a Complex Advanced Persistent threat should be included in the Incident Report.

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

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

Note that the initial part of an investigation is sometimes referred to as Triage.

8. Consideration 7. Recovery.

Once a thorough investigation has been carried out, recovery is a significant step for restoring whatever services or materials might have been affected during an incident. This could be the task of the technical people in the team. 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.

It is important that after an incident has been contained, key components that contributed to the incident should be eliminated. For example, when returning a compromised machine to production, is it acceptable to clean infection residue or should the machine in question be wiped cleaned, formatted and rebuilt from known reliable media?

Other practical recovery responses can include:

- Conducting a malware scrutiny.
- Allowing sufficient time to elapse to prove that a compromised network is now secure.
- Removing temporary constraints placed during the investigation period.
- Confirming the integrity of business systems and controls.
- Replacing compromised records with reliable versions
- Resetting passwords on compromised accounts.
- Installing updates and patches.
- Install or replace equipment that are susceptible to exploits.

The overall objective of the recovery process in **Incident Response** is to reinstate systems to normalcy , affirm that the systems are functioning normally, and repudiate all known vulnerabilities to prevent similar incidents from reoccurring.

9. Consideration 8. Documentation and Reporting.

Reporting an incident is more than sending an email or other notification to team members or relevant stakeholders. 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.

Reporting and documentation is a critical action that will always occur before, during and after Incident Response. Some key actions, events and processes that would require documentation has been highlighted in previous sections of this document. Emphasis should be laid on the following questions when documenting Incident Response Report.

- The date, time and actual location of the incident.
- Who discovered and reported the incident.
- Systems, materials , processes or Information affected.
- Stakeholders involved in the incident.
- Comprehensive description of what transpired.
- Who has been informed about the incident and action steps taken.

Some other points to consider in reporting and documentation is briefing the management about the incident in a timely fashion. Management should be notified immediately when an important incident is detected. Briefing is a critical action in reporting as it provides the management an overview of the situation which can help define the obligatory course of action.

As more information becomes available throughout the response process, additional briefings and updates should occur at regular intervals.

Sharing Information with internal and external stakeholders.

Sometimes, there is a considerable amount of information generated from incidents that occur within an organization and you can share information with external vendors or trusted service providers in a bid to educate them and also receive helpful information from them when the need arises.

Note that sharing information should be on a 'need to know' basis and it is advisable for organizations to involve the Legal Counsel expert when creating reports so that factors such as regulatory obligations, contractual obligations, and insurance obligations are properly considered as an incident investigation proceeds. All team members should be trained in a common lexicon of language to guarantee prompt and clear communication during incident response.

10. Consideration 9. Process Review.

It is imperative to continuously monitor an incident and the workload/performance of the team or Incident Handler. When you review an incident comprehensively you can make intelligent decisions about the factors listed below.

- 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 ?

Other activities that should also be considered during a process review is keeping a Lessons Learnt log.

The lessons can be positive or negative in nature but they should be current and relevant and ensure the maturity of your team over time. You might want to keep versions of the log so that you can keep track of its development and know which previous lessons learned were either integrated successfully and which needs to be revisited.

11. Consideration 10. Practice , Practice , Practice.

Do not wait until an incident occurs before you put your team to work. Once the organization has a workable plan in place, it is advisable to run through part or all of it as a tabletop exercise. Assemble the various stakeholders and talk through different scenarios and how the group would react. Document the results of these exercises and incorporate the findings into your plan.

When new resource persons join your **Incident Response** team, it is important that they understand how important these 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.

Your objective is not to intimidate the team members or peers but to determine if your plan works or not before the real event occurs. Drills and practices also reveal where lapses are and they can be resolved before real life scenarios happen.

12. Conclusion

An incident is considered to be any adverse event that threatens the progress, integrity or availability of your organization's objectives or resources. Encourage your **Incident Response** Team to take part in external events, such as by attending conferences, enrolling in training and other helpful activities.

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 fundamental business or service delivery can be endangered when incidents occur. It is the mandate of an efficient **Incident Response** Team to prevent , handle, resolve and adequately document incidents that may arise.

Incident Recovery is a significant tool of overall governance and to have it, in whatever form or shape, is a necessity. This fact is acknowledged and supported in the ISO 27001 security standards and in frameworks such as ITIL and COBIT.

References.

1. An empirical study on the use of the Generic Security Template for structuring the lessons from information security incidents. 2014. By Ying He, Chris Johnson, Karen Renaud ,Yu Lu and Salem Jebriel. School of Computing Science University of Glasgow, Glasgow, UK
● URL: http://www.researchgate.net/profile/Ying_He14/publication/262300500_An_empirical_study_on_the_use_of_the_Generic_Security_Template_for_structuring_the_lessons_from_information_security_incidents/links/5433e19c0cf2dc341dae01aa.pdf
2. Top Considerations for Incident Response co-authored by Tom Brennan of ProactiveRISK by Legal Sec
● URL: <http://www.proactiverisk.com/wp-content/uploads/2015/06/IR-Guidance.pdf>
3. Information Security Incident Reporting Policy by Herefordshire Council , 2013
4. Good Practice Guide for Incident Management by ENISA , 2010.
● URL: <https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management>
5. Local Government Cyber Security :Cyber Incident Response Guide,A Non-Technical Guide Essential for Elected Officials ,Administrative Officials and Business Managers by MS-ISAC
● URL: <http://msisac.cisecurity.org/members/local-government/documents/finalincidentresponseguide.pdf>