

# Response Preparation for Action

Reading

1h - 1h30m



Status

Incomplete

## Introduction

With any IR plan, there must be clear protocols in place for when an attack is taking place, and as security professionals, actions need to be taken. In the event that an attack develops into an incident, the team must have ready access to the detailed protocols that will help them pinpoint the problem, contain it, and put an end to it.

There are three key protocol development areas, which are, preparation for action during, after an incident, and before an incident. Beyond developing this plan, it is essential to test, rehearse, train, and maintain in order for the IR to be effective.

## Reading

### Preparation for Action "During the Incident"

Most planning tasks benefit from starting with the goal in mind. But when it comes to IR, you start in the middle, with the actual event response. The "during the event" stage represented below is the most crucial part of the IR strategy. In the event that an attack develops into an incident, the team must have ready access to the detailed protocols that will help them pinpoint the problem, contain it, and put an end to it. This team is called the Computer Security Incident Response Team (CSIRT).

To prepare, both the IRPT and members of the CSIRT must go through every possible outcome of an attack scenario and formulate a plan of action.

### CSIRT Trigger Events

In this first section, you will examine the event that sets in motion the CSIRT and the IR strategy. This set-off might be triggered by any of the following events or conditions:

- Detection of malware or malicious activity on a network or system
- Unusual network traffic or network congestion
- Unauthorized access or attempted access to sensitive data
- Suspicious user behavior, such as repeated failed login attempts
- Loss or theft of equipment or data
- Disruption of essential systems or services
- Natural disasters or other events that threaten the physical security of the environment
- Compliance violations or regulatory breaches
- Cyberattacks or attempted cyberattacks

- Detection of vulnerabilities or potential security weaknesses in the system

Following the submission of an indication, the IR team leader or the IR duty officer will decide whether or not to activate the IR plan. An IR duty officer, who is also a part of the CSIRT, reviews reports of unfavourable occurrences to verify or reject their authenticity as incidents. This person then alerts the CSIRT and initiates the IR plan after concluding that a real incident has occurred or is still occurring.

Every incident is unique, and there is a distinct set of abilities required for each potential emergency. It is for this reason that it's up to the IRPT to figure out who and what kind of resources are required to deal with each possible outcome of an attack scenario. For example, responding to a **denial-of-service (DoS)** attack or an internal virus infection, may need quite different expertise compared to dealing with a physical security issue.

After identifying each possible skill set combination, an IR plan section may be created specifically for that kind of attack. Moreover, the IR strategy should name a team leader for the situation at hand. If the event starts to get out of hand, the head of the CSIRT will keep adding people and tools until they've done all they can. The scribe (or historian) for the event should be named in the IR strategy in addition to the leader. This person is in charge of creating and updating an events log that will be used in the after-action review.

The next step in IR planning is to figure out what has to be done in light of the situation. Here is a specific example, the detection of malware on a network or system. The first step would be to verify the existence of a virus using antivirus software, system logs, or other monitoring systems. From there, finding out how vulnerable a system is to malware is the next step once an attack has been confirmed.



Are there just a few infected machines, or has it spread?

As soon as the scope is known, the team may begin trying to quarantine the virus, in this instance by isolating affected devices from the network and then checking for further signs of propagation. Additional procedures, like isolating network segments, cancelling server sessions, cutting the Internet connection, and even shutting down the network servers, may be required if isolating infected workstations does not stop the spread. Disinfecting computers by using antimalware software, checking for spyware, and so on would be the last step of operations during this example incident. The action during phase is finished when all traces of contamination have been wiped off.

## Preparation for Action "After the Incident"

The next protocol that needs to be developed for an IR plan is the preparation for action, after an incident has taken place. After the incident is controlled, the damage is evaluated, data is recovered, systems are cleaned of infection, and everything is returned to normal; then, the IR strategy needs to be reviewed and evaluated. The "after the incident" IR strategy must include the steps needed to recover from the most probable incident situations. It should also include forensics investigation, follow-up incident protection, and after-action evaluation.

## Forensic Analysis

The terms **forensic analysis** or **forensic investigation** refer to the methodical examination of data assets for evidence that may explain what happened. This investigation is particularly important after an incident, as the risks of further attacks increase due to the fact that details and vulnerabilities of these systems could be shared by any parties involved. Forensic investigation may help a company avoid future incidents by revealing and fixing potential entry points hackers might use. Unknown vulnerabilities or exploits may be better understood if you know which system was affected initially or how a certain attacker accessed the network. Information discovered during a forensic analysis may be used as evidence in a civil or criminal case, so it's important to be sure the person doing the study has the proper training.

## Closing the Incident

After an incident, the CSIRT must debrief by discussing what went wrong and what might have been done differently. The IR paperwork is double-checked for accuracy by all important players, who go over their notes. The team as a whole discusses what they did during the event and how well the IR plan functioned or failed to function, as well as what may be done differently. After

this debrief and discussion, the IR strategy may now be revised accordingly. The After Action Report (AAR), or sometimes referred to as Post-Mortem Review (PMR), may also be used as a training scenario for new team members. When the AAR/PMR is sent to management, the event is considered resolved, and the CSIRT may go into a dormant state.

## Preparation for Action "Before the Incident"

As introduced previously, planning well before an event occurs means that IR planners must use hardened information technology and security procedures. However, there may be unique aspects of each instance that call for individualized approaches to prevention. As part of the "before actions," the IR team, and other relevant personnel, take whatever precautions are necessary to mitigate the dangers posed by a specific attack. The only way for a team to always be prepared to reply to attacks is to practice their response repeatedly. Training the CSIRT, conducting IR plan tests, deciding on and keeping up with CSIRT tool selection, and educating end-users on the organization's policies and procedures are all part of this process.

## Planning, Testing, and Rehearsing

There must be participation from all users and management, as well as the IRPT and CSIRT, in testing, training, and exercising the IR plan once it has been created. The IR team (IRT) undergoes extensive training and certification, including the documentation of all incident response processes. Testing is an evaluation of the IR team's performance and capabilities under simulated attack scenarios, whereas training is the process of delivering knowledge and skills to the people responsible for executing the IR strategy. To make sure everyone is familiar with their responsibilities and to review and adjust the plan as needed, it is important to exercise it in a less stressful setting.

The IRPT's principal duty is to make sure the CSIRT is ready for any incident that may arise. In order to ensure an adequate level of preparedness, there has to be a lot of practice and training.

## Training the Stakeholders

The IRPT's principal duty is to guarantee that the CSIRT is ready to handle any incident that comes its way. This calls for a substantial amount of regular practice and rehearsal. There are several approaches that may be used while training IR staff, some examples of this training include:

- **Phishing simulation:** simulate phishing attacks to educate users on how to identify and respond to suspicious emails.
- **Security awareness training:** training on security best practices, such as how to create strong passwords, how to identify and report suspicious activity, and how to protect sensitive information.
- **Role-playing exercises:** exercises to simulate different types of security incidents and train users on how to respond.
- **Tabletop exercises:** exercises that simulate IR scenarios and test the readiness of the IRT and the organization as a whole.
- **Hands-on training:** training for users on the use of security tools, such as anti-virus software, firewalls, and intrusion detection systems.
- **Sharing real-life examples and case studies:** examples of security incidents and how they were handled to educate users on the importance of IR and what to expect.
- **Encourage reporting:** encourage users to report any suspicious activity or security incidents they come across and make it easy for them to do so.
- **Regular reminders:** send regular reminders and updates to users on the importance of IR and the measures they can take to protect themselves and the organization.

Overall, IRe training for end users should be ongoing, interactive, and tailored to their specific roles and responsibilities. It's important to regularly update the training as new threats emerge, and to provide multiple channels for users to access the training.

## IR Plan Testing

The testing phase of IR planning is essential. Few plans can be carried out exactly as they were drafted, they need testing to reveal loopholes, errors, and unnecessary steps. The testing phase reveals flaws, which need to be addressed, resulting in a final plan that can be depended upon in an emergency. Common methods for trying out backup plans consist of:

- **Tabletop exercises:** this is a type of training where a group of people simulate a response to a hypothetical incident, usually in a conference room setting. This allows the IRT to practice their roles and procedures in a controlled environment, and to identify and address any weaknesses in the plan.

- **Walk-through exercises:** this is a type of training where the IRT walks through the steps of the plan, discussing each step and identifying any potential issues. This allows the IRT to become familiar with the plan and to identify any areas that need improvement.
- **Full-scale exercises:** this is a type of training where the IRT actually carries out the plan in a simulated real-world scenario. This allows the IRT to practice their roles and procedures in a realistic environment, and to identify and address any weaknesses in the plan.
- **Penetration testing:** this is a type of testing where a third-party is hired to simulate a cyber attack on an organization's systems to identify vulnerabilities in the organization's security. This can help to identify any weaknesses in the IR plan and to test the organization's ability to respond to a real-world attack.
- **Red teaming:** this is a type of testing where a group of experts simulate an attack on an organization's systems and infrastructure to identify vulnerabilities in the organization's security. This can help to identify any weaknesses in the IR plan and to test the organization's ability to respond to a real-world attack.
- **War-gaming:** this is a type of testing where a group of experts simulate a complex and realistic incident to test an organization's IR plan and to identify any weaknesses or gaps. This can help to identify any weaknesses in the IR plan and to test the organization's ability to respond to a real-world attack.

It's important to note that testing CPs should be done regularly, and plans should be updated and refined based on the results of the testing. Also, it's important to include a wide range of scenarios in your testing, to ensure that your IR plan can handle different types of incidents.

## IR Plan Maintenance

The IR strategy must be formally maintained, just like all other plans and policies inside the firm. The plan should contain a defined timeline for revisions and a written method for reporting difficulties. Any member of the company should be able to provide suggestions for improvement, and report mistakes or inaccuracies in procedures to the IRPT using a system built within the revision process.

The IRPT has to gather this information and include it into their regular updates to the IR strategy. The strategy should be examined and updated at least once a year. Reviewing the plan right after a test or training session is also recommended since such activities often reveal flaws in the present strategy and provide insight into how to fix them.

The process of testing does not end with the creation of the final plan. The IR plan should be checked at least twice a year, once with an organized walk-through exercise and once with a more realistic sort of exercise if feasible. Assuming no changes were made to the IR plan during the after-action assessment, it stands to reason that the portions utilized during the response may not need to be tested at the same frequency going forward. Additional testing of revised plans should be undertaken as soon as possible.

When all the parts of the IR plan have been written and tested, the final IR plan document may be made. The structure and details of an IR strategy are, of course, up to the discretion of each individual company. The primary condition is that an IR strategy be created, practiced, and stored in a convenient area. Here is a list of recommendations on how to build a copy of an IR plan that will be easy to locate and use in an emergency:

- **Keep it up to date:** the IR plan should be reviewed and updated regularly to ensure that it remains relevant and effective.
- **Make it easily accessible:** the IR plan should be kept in a central location that is easily accessible to the IRT, such as a binder in a designated location or a digital copy that can be easily accessed from any device.
- **Use clear and consistent formatting:** the IR plan should use clear and consistent formatting, including headings, bullet points, and numbered lists to make it easy to locate and follow the information.
- **Include contact information:** the IR plan should include a list of key contacts, including the IRT, senior management, and external partners and vendors.
- **Include an IR checklist:** the IR plan should include a checklist of the steps that need to be taken in the event of an incident, to help guide the IRT through the process.
- **Include instructions for activating the plan:** the IR plan should include clear instructions on how to activate the plan, including who is responsible for doing so and the criteria for activating the plan.
- **Use diagrams and flowcharts:** the IR plan should include diagrams and flowcharts to help illustrate key processes and procedures, making it easier for the IRT to understand and follow.
- **Test the plan regularly:** the IR plan should be tested regularly, through tabletop exercises and other training, to ensure that it is effective and that the IRT is familiar with its contents.
- **Make it available in different formats:** the IR plan should be available in different formats, such as hard copy, digital, and mobile-friendly, to ensure that it can be accessed by all members of the IRT, regardless of their location.

- **Keep a copy in a disaster recovery location:** the IR plan should be stored in a disaster recovery location, such as a different building or a cloud-based storage, to ensure that it can be accessed in the event of a disaster or an emergency.

With each adjustment, whether planned or unplanned, the updated plan is sent out to the whole IRPT and top management for feedback. The IRPT will have a second meeting when everyone has had a chance to study the updated version for final approval. The plan is updated and republished with a new effective date and revision date.

## Key Takeaways

- Approaching an IR plan with the order of preparation for action during, after an incident, and before an incident helps create a better and more reliable IR plan.
- In order for a plan to be reliable, it needs to be tested regularly and rehearsed to ensure all those involved are able to execute the plan effectively when needed.
- Training is a vital part of any plan and should be both comprehensive and inclusive of all key stakeholders and possible incident scenarios.
- Any plan that has been developed requires ongoing maintenance. This is required to keep plans in compliance and functional, as well as to adapt them to changing circumstances.

## Conclusion

IR planning and policies are no small task. These large and complex plans require multiple teams, stakeholders, training, rehearsing, and maintenance in order to be effective. However, when done correctly, it provides an organization with a concrete plan of action to ensure a secure and defensible IT infrastructure.

✓ Mark Completed

←

Previous  
Pre-Incident Planning

Next  
Planning and Building CSIRT

→

### How well did this activity help you to understand the content?

Let us know how we're doing



## W05D5

Fri Jul 26

> Lectures (1)







✓ Work (9)

8 hrs

</> Case Study: Vulnerability Assessment Report

⚡ Peer Review: Assessment Report Briefing

</> Project: Cat's Company Vulnerabilities

-  [Course Reflection](#)
-  [Overview - Incident Response](#)
-  [Introduction to Incident Response](#)
-  [Pre-Incident Planning](#)
-  [Response Preparation for Action](#)
-  [Planning and Building CSIRT](#)

> **Other** (1)

[W05D5 Schedule »](#)