Pre-Incident Planning

Reading

40m

Status | Incomplete

Introduction

Incidents, whether malicious in nature or not, should be expected by Cyber Security professionals. The best mindset is to always anticipate and be prepared with a well-thought-out IR plan.

But how do you create an IR plan? While each organization is unique, there is a recommended process that can be applied to support the creation of an IR plan which ensures the correct individuals are involved, and risks can be effectively mitigated. In short, the steps taken in preparing for an incident are just as important as the IR itself.

Reading

IR Planning Process

When creating an IR plan, there are nine steps which information security professionals can use from draft to implementation.

The IR planning process is as follows:

1. Gather a team and form the IR Planning Team (IRPT)
2. Draft the IR plan
3. Develop a business impact assessment/risk assessment as part of the incident response process
4. Determine remediation measures or controls
5. Create a group to deal with Cyber Security incidents, usually referred to as the computer security incident response team (CSIRT) (covered subsequently)
6. Develop IR plans and methods (covered subsequently)
7. Prepare the IR plan
8. Make sure to schedule time for testing, training, and practice
9. Periodically update the plan

Step 1: Gather a Team (IRPT)

The first step in this process is to organize what is known as the **Incident Response Planning Team, or IRPT**. The IRPT is responsible for the development and administration of the IR plan.

The Incident Response Planning Team should include the following Stakeholders:

- **Senior Leadership Team (SLT)**, which oversees the team's work and ensures that it is completed in a timely manner. The SLT also needs to know what IR teams do and must preauthorize IRPT, an essential business function engagement to stop an incident's spread and effect.
- **IT management**, which must know what resources and access IR teams need to prepare for and react to events.
- The **security team**, which will plan for an attack on the network and develop a response based on the vulnerabilities discovered.
- A **legal representative**, who will ensure that any response is in compliance with relevant laws and regulations.
- A **communications representative**, who will ensure that all communications are accurate and professional.

The IR policy, strategy, and procedures will be developed with input from the IRPT. The group will need a champion, usually the chief technology officer (CTO), chief information security officer (CISO), or vice president of IT, and a recruited or elected group leader to administer the team, much like any other organisational team.

To establish the IR policy and ultimately the IR strategy, the committee should have frequent meetings. At the proper time in the planning process, this team is also accountable for the incident response organisational framework, development, and training. Its responsibility includes making sure the plans are kept up to date.

Step 2: Draft the IR plan

After the IRPT is formed, the next step is to begin drafting the Incident Response plan (IR plan).

As part of the IR plan, the IRPT must design three incident-handling protocols for each probable attack scenario. These procedures cover before (anticipation), during, and post-incidents:

- **Pre-incident** - in this part of the IR plan, the IRPT creates incident-preparation methods. These methods could include data backup, training, testing, service agreements, off-site data storage, and cloud computing services.
- **During the incident** - for this stage the IRPT creates and records urgent response protocols for individuals, groups, or specific roles. This must include function-specific procedures for managers, firewall administrators, and systems administrators. A scribe or secretary must record every action.
- **Post incident** - after the incident procedures are created, planners construct and record the immediate post-incident processes. Again, methods may vary by functional area, so it is important to understand the type of company you are creating these procedures for.

> You will examine these in more detail in the next reading.

Activating the plan

In addition to these three stages of an IR plan, the company should outline the conditions under which the IR plan will be activated in advance in order to minimise the likelihood of business disruption and data loss.

For a threat to be considered an information security event, it must meet the following criteria:

- Specifically, it targets the company's information assets.
- There is a reasonable possibility of it succeeding.
- It poses a risk to the privacy, security, or availability of data and digital assets.

Further Reading

> **Add depth to your understanding**
>
> Read the article below and add notes about the key points to your PKM. Make note of any templates and examples you think might be useful.

[Incident Response Plan 101: The 6 Phases, Templates, and Examples]

Key Takeaways

- Regardless of the unique nature of the organization, there are clear steps involved in developing IR Policies and Plans to ensure a robust IR plan is developed.
- Essential to any IR plan is the formation of the IRPT. The IRPT is responsible for the development and administration of the IR plan and consists of individuals from across the organization.
- As part of the IR plan, the IRPT must design three incident-handling protocols for each probable attack scenario. These procedures must cover pre-, during-, and post-incident processes.

Conclusion

While an IR plan is an essential action for any organization, it is only as effective as the planning and procedure put in place. Next, we'll build on this knowledge and explore Incident Response Preparation for Action.

✓ Mark Completed

Previous
Introduction to Incident Response

Next
Response Preparation for Action

? Planning and Building CSIRT

› Other (1)

W05D5 Schedule »