ICE'S ULTIMATE GUIDE TO

ESTABLISHING AN INCIDENT RESPONSE PLAN

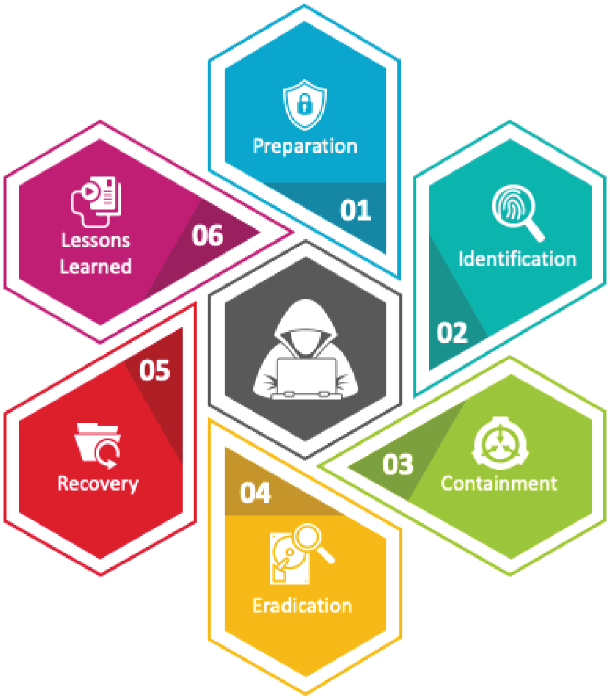
ICE

TRUSTED IT PARTNER

WHAT IS AN INCIDENT RESPONSE PLAN?

An incident response plan (IRP) is a set of protocols that outline the measures to be done during the incident response process.

This procedure enables an organization to respond to cybersecurity events quickly and effectively, enabling successful containment as well as the creation of a plan to make sure the incident won't happen again.



WHAT ARE THE SIX PHASES OF INCIDENT RESPONSE?

Generally, the incident response phases are:

1. Preparation

- Establish a plan and prepare with triage exercises

2. Identification

- Identify the size and scopr of an attack, so that a response can be prioritized appropriately

3. Containment

- Isolate compromised devices

4. Eradication

- All threats

5. Recovery

- Restore normal services

6. Lessons Learned

- Analyze relevant information to prevent the recurrence of the incident, assess response, etc.

WHAT SHOULD BE INCLUDED IN AN INCIDENT RESPONSE PLAN?

Any incident response plan should set out a targeted, distinctly organized strategy for handling a wide range of cybersecurity situations. Each incident response plan will be distinctive because each organization's structure, size, and varied functions are distinct, and a general, one-size-fits-all strategy simply won't do.

AN INCIDENT RESPONSE PLAN'S FUNDAMENTAL COMPONENTS ARE:

1. Mission and goals
2. Roles and responsibilities of the critical incident response team
3. Documentation of preparation for cyberthreats
4. Documentation of the process for identifying a critical incident
5. Criteria for when a critical incident will be declared
6. Processes for mitigation and containment
7. Rapid recovery plans
8. Post-incident evaluation and review

1. Mission and goals

To be as effective as possible, a solid critical event response plan should be built upon a number of high-level objectives.

Begin your IRP with a mission statement that is:

- Simple
- Actionable
- Inclusive of and agreed to by all relevant stakeholders
- Practical
- Flexible and routinely updated

2. Roles and responsibilities of the critical incident response team

The duties and responsibilities of your incident response team during an attack should also be included in an IRP. Important duties should be assigned to specific people, and the documentation in this portion of the IRP should contain the following:

- The members of the incident response team (we will examine this in detail in an upcoming section)
- The procedures and essential contacts for coordinating with the executive management, legal team, public relations team, and cybersecurity suppliers of your organization
- The procedures and main contacts for contacting clients, business partners, vendors, and/or staff as necessary
- If necessary, a system to quickly automate responses to relevant cybersecurity and/or data privacy regulations, such as the GDPR and CCPA

The incident response team may be made up of full-time incident response staff in larger organizations; full-time incident response staff may make up the team in smaller businesses. Whatever organizational structure your company chooses, your IR team should include the following crucial positions:

- Incident response managers: Approve the final plan and coordinate action when an incident takes place
- Security analysts: Review security alerts, pinpoint potential incidents, and investigate an attack to better grasp its scope
- Threat researchers: Obtain contextual information relevant to a given threat, gathering details from the web, security data, threat intelligence feeds, and other trusted sources
- Additional stakeholders: Can include senior management, human resources staff, public relations staff, and/or senior security employees
- Third parties: Can include cybersecurity service providers, legal counsel, and/or law enforcement

Although existing internal workers can be used to create an incident response team, an increasing number of businesses are choosing to centralize their efforts by working with cyber incident response providers.

3. Documentation of preparation for cyberthreats

You will describe the procedures used to anticipate, stop, and respond to cybersecurity assaults in this section of an IRP, including:

- Cybersecurity awareness training efforts
- An overview of the primary cyber threats most likely to impact your organization
- Policies for responding to cybercriminal demands, such as payments made to attackers

4. Documentation of the process for identifying a critical incident

Additionally, there must to be a thorough procedure for spotting possible incidents, one that emphasizes taking rapid action. Keep records of these detecting techniques:

- Methods for processing security alerts delivered by a variety of systems, such as intrusion detection, security information/event management, etc.
- User reporting procedures for suspicious activities and assault attempts
- A method of escalation that makes it evident how to prioritize serious threats