# Security Incident Response Plan

Security Incident Response Plan (SIRP) using the four phases: Preparation, Detection and Analysis, Containment and Eradication, and Recovery, and Lessons Learned.

1. **Preparation Phase**

*A. Define the scope and objectives of the SIRP* - (SIRP) defines the types of security incidents that the plan covers and the resources and systems that are within the scope of the plan. The scope may include information systems, networks, applications, data, physical facilities, and personnel.

The objectives of a SIRP are to establish a framework for responding to security incidents in a timely and effective manner.

1. Minimizing the impact of security incidents on the organization's operations, assets, and reputation.
2. Preventing the escalation of security incidents.
3. Identifying the root cause of security incidents and implementing corrective actions to prevent similar incidents from occurring in the future.
4. Complying with legal and regulatory requirements related to incident response and reporting.
5. Providing clear and consistent guidance to the incident response team on how to respond to security incidents.
6. Enhancing the organization's security posture by improving incident response capabilities.
7. Establishing communication protocols and contact lists to ensure that all stakeholders are informed of security incidents and the response efforts.
8. Regularly reviewing and updating the SIRP to ensure it remains relevant and effective in addressing current and emerging threats.

*B. Establish an incident response team (IRT) -* IRT is responsible for responding to security incidents, mitigating their impact, and restoring normal operations as quickly as possible.

1. Identify key stakeholders: Determine the stakeholders who will be involved in the incident response process. These may include IT staff, security personnel, legal, communications, and other relevant teams within the organization.
2. Define roles and responsibilities: Clearly define the roles and responsibilities of each team member to ensure that everyone understands their specific duties during an incident.
3. Determine the size of the team: Determine the appropriate size of the IRT based on the organization's size, complexity, and the types of incidents that may occur. It is important to ensure that the team is large enough to handle all potential incidents, but not so large that coordination becomes difficult.
4. Select team members: Select team members who have the necessary skills, experience, and knowledge to respond to incidents effectively. The team members should be able to work well together, remain calm under pressure, and make sound decisions quickly.
5. Establish communication protocols: Establish communication protocols for the IRT to ensure that team members can communicate with each other effectively and efficiently during an incident. This may include setting up a communication channel, such as a group chat or conference call, and determining who is responsible for communicating with external stakeholders, such as management or law enforcement.
6. Provide training and testing: Provide regular training and testing to the IRT to ensure that team members understand their roles and responsibilities, are familiar with the incident response process, and are prepared to respond to incidents effectively.

*C. Develop communication protocols and contact lists -*  Developing communication protocols and contact lists is an essential part of the SIRP to ensure that everyone involved in the incident response is aware of their roles and responsibilities.

Here are some steps you can follow to develop communication protocols and contact lists:

1. Identify key stakeholders: The first step is to identify the key stakeholders who will be involved in the incident response. This may include the IT team, the security team, management, and external stakeholders like vendors or partners.
2. Determine communication channels: Next, determine the communication channels that will be used to report and respond to security incidents. This may include email, phone calls, messaging apps, or other collaboration tools.
3. Define communication protocols: Once the communication channels are identified, define the communication protocols that will be followed during incident response. This should include who will be responsible for communicating updates, how often updates will be provided, and what information will be shared.
4. Develop contact lists: Create a comprehensive contact list that includes the names, roles, contact information, and availability of all stakeholders involved in incident response. This list should be regularly updated and shared with all parties involved.
5. Test and refine: Finally, test the communication protocols and contact lists by conducting regular drills or tabletop exercises. This will help identify any gaps or weaknesses in the incident response plan and allow for necessary adjustments.

*D. Prepare a list of critical assets and their owners -* it is important to prepare a list of critical assets and their owners. This list will help to identify the assets that need to be protected and the individuals or teams responsible for their management and security.

1. Identify critical assets: Start by identifying the critical assets in your organization. These may include hardware, software, data, or other resources that are essential to your business operations.
2. Categorize assets: Categorize the assets into different groups based on their criticality and sensitivity. This will help you prioritize your incident response efforts.
3. Identify asset owners: For each asset, identify the owner or custodian responsible for its management and security. This may include IT staff, business unit managers, or other individuals.
4. Document ownership information: Document the contact information for each asset owner, including their name, title, department, and contact information. This information should be updated regularly.
5. Establish communication protocols: Establish communication protocols for contacting asset owners in the event of a security incident. This may include a designated point of contact or a predefined communication channel.
6. Test and refine: Regularly test and refine your list of critical assets and their owners to ensure it remains up to date and relevant to your organization's needs.

*G. Develop a risk assessment process to identify potential security incidents* - Developing a risk assessment process is an essential step in creating a comprehensive Security Incident Response Plan (SIRP). This process will help you identify potential security incidents and prioritize your incident response efforts.

1. Identify potential risks: Start by identifying the potential risks to your organization's security. This may include threats from external attackers, malicious insiders, or accidental incidents.
2. Determine the likelihood and impact of each risk: For each potential risk, determine the likelihood of it occurring and the impact it would have on your organization if it did occur. This will help you prioritize your response efforts.
3. Define risk management strategies: Define strategies for managing each potential risk. This may include implementing security controls, performing regular vulnerability assessments, or developing incident response plans.
4. Assign responsibility for risk management: Assign responsibility for managing each risk to a specific individual or team. This may include IT staff, security personnel, or business unit managers.
5. Monitor and review: Monitor the effectiveness of your risk management strategies and review them regularly to ensure they remain up to date and effective.
6. Continuously improve: Continuously improve your risk assessment process by incorporating feedback and insights from incident response activities and other security-related events.

*H. Establish a procedure to classify the severity of incidents* - Establishing a procedure to classify the severity of incidents is an important step in creating a comprehensive Security Incident Response Plan (SIRP). This procedure will help you prioritize your incident response efforts and ensure that the appropriate resources are allocated to each incident.

1. Identify incident categories: Start by identifying the categories of incidents that are relevant to your organization. This may include malware infections, unauthorized access attempts, data breaches, or other types of incidents.
2. Define severity levels: Define severity levels for each incident category. This may include levels such as low, medium, and high, or more specific levels based on the potential impact of the incident.
3. Establish criteria for severity levels: Establish clear criteria for each severity level based on the impact of the incident on your organization. This may include factors such as the extent of the compromise, the sensitivity of the data involved, or the potential for financial or reputational damage.
4. Assign incident response teams: Assign incident response teams to each severity level based on their level of expertise and the resources required to respond to each incident.
5. Develop response procedures: Develop response procedures for each severity level based on the assigned incident response teams and the severity criteria. This should include clear instructions for initiating incident response, containing and mitigating the incident, and restoring normal operations.
6. Continuously review and update: Continuously review and update your severity classification procedure based on feedback and insights from incident response activities and other security-related events.

*I. Develop a playbook for responding to different types of security incidents* - Developing a playbook for responding to different types of security incidents is an important step in creating a comprehensive Security Incident Response Plan (SIRP). A playbook is a set of detailed procedures and guidelines that outline the steps to be taken in response to a specific type of security incident.

1. Identify incident types: Start by identifying the different types of security incidents that may occur in your organization. This may include malware infections, phishing attacks, data breaches, physical security breaches, and more.
2. Analyse incident characteristics: Analyse the characteristics of each type of incident, including the potential impact, the attack vectors, and the likely sources of the attack. This will help you develop a playbook that is tailored to the specific incident type.
3. Develop response procedures: Develop detailed response procedures for each incident type, including clear instructions for initiating incident response, containing, and mitigating the incident, and restoring normal operations.
4. Assign roles and responsibilities: Assign specific roles and responsibilities for each incident type, including incident response team members and stakeholders who should be informed about the incident.
5. Test and refine: Test each playbook through simulations and tabletop exercises, and refine the procedures based on the results.
6. Continuously update: Continuously update the playbooks based on feedback and insights from incident response activities and other security-related events.
7. **Detection and Analysis Phase**
8. *Establish a process for detecting security incidents -*
9. Identify key assets: Start by identifying the key assets that need to be protected. These could be servers, databases, applications, or any other system that is critical to your organization's operations.
10. Define incident types: Next, define the types of security incidents that are most likely to occur. This could include malware infections, phishing attacks, unauthorized access, or data breaches.
11. Configure monitoring: Use SIRP to configure monitoring and alerting for the identified incident types. SIRP allows you to set up automated alerts based on specific conditions, such as failed login attempts or changes to critical files.
12. Define response procedures: Establish response procedures for each incident type. This should include the steps to take when an incident is detected, such as isolating affected systems, conducting a forensic investigation, and notifying relevant parties.
13. Test the process: Once you have established your incident detection and response process, test it regularly to ensure it is effective. This could involve running simulations or tabletop exercises to identify areas for improvement.
14. *Determine the severity and impact of the incident* - When an incident occurs, it is important to assess the severity and impact of the incident as part of the initial response.

* Severity refers to the level of impact of the incident, which can be determined by evaluating the potential harm to the affected system, data, or infrastructure. This can include the scope and magnitude of the incident, the number of systems or users affected, and the criticality of the impacted systems or data.
* Impact refers to the consequences of the incident, which can be assessed by examining the potential damage to the organization's reputation, financial losses, regulatory non-compliance, or legal liabilities. The impact can also include the potential disruption to business operations, loss of productivity, and the need for additional resources to mitigate the incident.
* To determine the severity and impact of an incident, the incident response team should gather all available information about the incident, such as the type of attack, the affected systems or data, and the potential impact on the organization. This information can be used to evaluate the incident and determine the appropriate response actions, such as containment, investigation, and remediation.
* It is also important to document the severity and impact of the incident as part of the incident response process. This documentation can help to improve the organization's incident response capabilities and to prepare for future incidents.

1. *Analyse the incident to determine the root cause and potential impact –*

Analyzing the incident involves gathering and reviewing all available information about the incident, including log files, system and network configurations, and any other relevant data. The goal of this analysis is to determine the root cause of the incident, which is the underlying reason that the incident occurred. This analysis can also help to identify any vulnerabilities or weaknesses in the organization's security posture that contributed to the incident.

Potential impact analysis involves assessing the potential consequences of the incident, such as the potential loss of data, intellectual property, or financial assets. The impact analysis should also consider any regulatory or legal requirements that may apply, as well as the impact on the organization's reputation and business operations.

To perform the root cause and potential impact analysis, the incident response team may use various tools and techniques, such as:

1. Forensic analysis: This involves analyzing system logs, memory dumps, network traffic, and other data sources to determine the source and scope of the incident.
2. Threat intelligence: This involves using information about known threats, vulnerabilities, and attacker techniques to help identify the root cause of the incident.
3. Vulnerability assessment: This involves evaluating the organization's systems and infrastructure for weaknesses that may have contributed to the incident.
4. Business impact analysis: This involves assessing the potential impact of the incident on the organization's business operations, financials, and reputation.
5. *Determine the appropriate response and level of escalation – Once* an incident has been detected, assessed, and analysed, the next step in a SIRP (Security Incident Response Plan) is to determine the appropriate response and level of escalation.

The response plan should be designed to address the specific type of incident and its severity and impact. The goal of the response plan is to contain the incident, minimize damage, and restore normal operations as quickly and efficiently as possible.

The appropriate response will depend on the nature and severity of the incident, but some common response strategies include:

1. Containment: This involves isolating the affected systems or network segments to prevent the incident from spreading further.
2. Eradication: This involves removing the cause of the incident, such as malware, and restoring the affected systems to a clean state.
3. Recovery: This involves restoring normal operations and data from backups, if available.
4. Investigation: This involves conducting a detailed investigation to determine the root cause of the incident and to identify any weaknesses in the organization's security posture.
5. Communication: This involves communicating with stakeholders, such as customers, partners, and regulators, to keep them informed about the incident and the organization's response.

The level of escalation will depend on the severity of the incident and the resources and expertise available to the incident response team. Escalation may involve notifying senior management, engaging external resources such as incident response service providers, or notifying law enforcement or regulatory agencies.

The incident response team should also document all aspects of the incident response process, including the response plan, response activities, and any communication or escalation efforts. This documentation will be useful for future incident response planning and to comply with any legal or regulatory requirements.

1. *Notify relevant stakeholders, including the incident response team, management, and affected parties -*

* Notifying relevant stakeholders is a critical part of any SIRP (Security Incident Response Plan) and should be done as soon as possible once an incident has been detected and assessed.
* Stakeholders that may need to be notified include the incident response team, management, and affected parties. Other stakeholders may include customers, partners, vendors, and regulatory agencies, depending on the nature and severity of the incident.
* The incident response team should be notified first, as they will be responsible for managing the incident response process. The incident response team should include experts from various departments, such as IT, legal, compliance, and public relations.
* Management should also be notified as soon as possible, as they will need to make decisions about the appropriate response and any necessary resources. Management should be kept informed throughout the incident response process.
* Affected parties, such as employees or customers, should also be notified as soon as possible, especially if their personal data or other sensitive information has been compromised. The notification should include information about the incident, the potential impact, and any steps that affected parties can take to protect themselves.
* When notifying stakeholders, it is important to communicate clearly and honestly about the incident, the potential impact, and the organization's response plan. The incident response team should also provide regular updates to stakeholders throughout the incident response process.
* In addition to notifying stakeholders, the incident response team should also document all aspects of the incident response process, including the notifications that were made and any responses received. This documentation will be useful for future incident response planning and to comply with any legal or regulatory requirements.

1. *Update the incident management system to track the incident and response -*

The incident management system is a tool used to manage incidents and should be updated regularly throughout the incident response process.

The incident management system should capture all relevant information about the incident, such as the date and time of the incident, the type of incident, the severity and impact, the root cause, and the response plan. It should also track the progress of the incident response, including any containment, eradication, recovery, or investigation activities that have been undertaken.

Updating the incident management system provides several benefits, including:

1. Providing a central repository of information: The incident management system provides a single source of truth for all incident-related information. This can help ensure that all team members are working from the same set of information and can reduce the risk of miscommunication.
2. Enabling collaboration: The incident management system can facilitate collaboration between team members by providing a platform for sharing information and tracking progress.
3. Supporting reporting and analysis: The incident management system can provide reports and analysis of incident-related data, which can help identify trends, areas for improvement, and opportunities for preventative measures.
4. Ensuring compliance: The incident management system can help ensure that the organization is complying with any legal or regulatory requirements by documenting all incident-related activities.
5. To ensure that the incident management system is updated effectively, the incident response team should establish clear processes and procedures for updating the system, including who is responsible for updating it and how frequently it should be updated.
6. **Containment and Eradication Phase**

*A. Implement temporary or permanent solutions to contain the incident* - The appropriate solutions will depend on the nature and severity of the incident, but some common containment strategies include:

1. Isolation: Isolating the affected systems or network segments to prevent the incident from spreading further.
2. Patching: Applying patches or updates to vulnerable systems or software to prevent the incident from reoccurring.
3. Disabling services: Disabling services or applications that may be contributing to the incident.
4. Blocking traffic: Blocking traffic from suspicious or malicious IP addresses or domains.
5. Reconfiguring systems: Reconfiguring systems to strengthen security controls or remove unnecessary access.
6. Implementing compensating controls: Implementing compensating controls to protect sensitive data or assets while the incident is being contained.

Temporary solutions are typically implemented to contain the incident quickly and reduce the immediate risk. Once the incident has been contained, the incident response team can assess the impact and determine whether permanent solutions are required.

Permanent solutions are typically more comprehensive and are designed to prevent similar incidents from occurring in the future. These solutions may include implementing new security controls, upgrading systems or software, or improving employee training and awareness.

It is important to note that any changes made to contain the incident should be documented in the incident management system and reviewed by the incident response team to ensure they do not introduce new risks or vulnerabilities.

Finally, the incident response team should regularly review and update the temporary and permanent solutions as part of their ongoing security management processes.

*B. Determine the root cause and implement corrective actions* - To determine the root cause of a security incident and implement corrective actions, the SIRP typically follows the following steps:

1. Identification and Containment: The first step is to identify the security incident and contain it to prevent further damage. This involves isolating affected systems, limiting user access, and blocking network traffic.
2. Investigation: The SIRP team investigates the incident to determine its scope, impact, and root cause. This involves reviewing system logs, analyzing network traffic, and conducting interviews with stakeholders.
3. Root Cause Analysis: Once the investigation is complete, the SIRP team identifies the root cause of the security incident. This could be a vulnerability in the system, a misconfigured firewall rule, or a phishing attack that exploited a user's credentials.
4. Corrective Action: Based on the root cause analysis, the SIRP team develops a plan to address the issue and prevent it from recurring in the future. This could involve patching vulnerabilities, updating policies and procedures, or providing additional security awareness training to employees.
5. Recovery: Finally, the SIRP team implements the corrective actions and monitors the system to ensure that the incident has been fully resolved. Once the system is deemed secure, it can be returned to normal operations.

*C. Communicate with stakeholders on the status of containment and eradication efforts* –

1. Keep stakeholders informed: It's important to communicate with stakeholders about the status of containment and eradication efforts in a timely and transparent manner. This helps to build trust and ensure that everyone is aware of what is being done to address the issue.
2. Provide regular updates: Stakeholders should be provided with regular updates on the progress of containment and eradication efforts. This could include daily or hourly updates, depending on the severity of the incident.
3. Use clear language: It's important to use clear and simple language when communicating with stakeholders. Technical jargon and complex explanations can lead to confusion and misunderstanding.
4. Be honest about limitations: It's important to be honest about the limitations of the SIRP process and any challenges that may arise. This helps to manage stakeholder expectations and avoid false promises.
5. Assign a point of contact: It's helpful to assign a single point of contact to communicate with stakeholders. This helps to ensure consistency in messaging and avoids confusion.
6. Ensure confidentiality: While stakeholders should be kept informed, it's important to maintain confidentiality and not disclose any sensitive information that could compromise the security of the system.
7. Prepare a communication plan in advance: In order to communicate effectively during a security incident, it's important to have a communication plan in place in advance. This plan should outline the stakeholders that need to be notified, the frequency of updates, and the methods of communication that will be used.

*D. Verify the effectiveness of containment and eradication measures* - verifying the effectiveness of containment and eradication measures during a security incident, the following steps can be taken as part of the SIRP:

1. Monitor the system: The SIRP team should monitor the affected system closely to ensure that the security incident has been contained and eradicated. This involves checking logs, analysing network traffic, and conducting scans for any signs of malicious activity.
2. Conduct testing: Once the system has been secured, the SIRP team should conduct testing to verify that the containment and eradication measures have been effective. This could involve running vulnerability scans, penetration testing, or other forms of testing to identify any remaining weaknesses or vulnerabilities.
3. Evaluate results: Based on the results of the testing, the SIRP team should evaluate the effectiveness of the containment and eradication measures. If any issues are identified, additional corrective actions may need to be taken.
4. Document the results: It's important to document the results of the testing and evaluation process. This helps to ensure that the SIRP team has a clear record of what was done, what worked, and what didn't work.
5. Share results with stakeholders: Once the testing and evaluation process is complete, the SIRP team should share the results with stakeholders. This helps to build trust and demonstrate that the security incident has been fully resolved.
6. Review and update the SIRP: Finally, the SIRP team should review and update the SIRP based on the results of the testing and evaluation process. This helps to ensure that the SIRP remains effective in responding to future security incidents.
7. **Recovery Phase**

*A. Develop a plan to restore systems and services to normal operations –*

1. Assess the situation: First, assess the extent of the damage or disruption to the systems and services. Determine the scope of the problem and identify the root cause.
2. Prioritize restoration: Next, prioritize which systems and services need to be restored first based on their importance to the business and the impact of their downtime.
3. Form a restoration team: Assemble a team of IT professionals with the necessary expertise to fix the problem. Make sure to include representatives from all affected areas of the business.
4. Develop a restoration plan: Create a detailed plan that outlines the steps necessary to restore the affected systems and services. Make sure to include contingency plans in case the initial plan doesn't work.
5. Communicate with stakeholders: Keep stakeholders informed of the restoration process and provide regular updates on progress. This includes both internal stakeholders, such as employees, and external stakeholders, such as customers and vendors.
6. Test and validate: Before returning systems and services to normal operations, thoroughly test and validate them to ensure they are functioning properly.
7. Monitor and evaluate: Once systems and services are restored, monitor them closely to ensure they remain stable and address any issues that arise.
8. Review and learn: Conduct a post-incident review to identify what went wrong, what worked well, and what could be improved in the future.

B. Validate and test restored systems and services.

**V. Lessons Learned Phase**

A. Conduct a review of the incident response process to identify successes and areas of improvement - To conduct a review of the incident response process to identify successes and areas of improvement

1. Define the objectives: Determine the goals of the review and identify what you hope to achieve. This may include identifying areas for improvement, assessing the effectiveness of the incident response process, and evaluating the response team's performance.
2. Gather data: Collect data related to the incident response process, including incident reports, log files, and other relevant documentation. This data will be used to evaluate the incident response process and identify areas for improvement.
3. Analyse the data: Review the data collected and analyze it to identify successes and areas for improvement. This may include identifying patterns or trends in incident response, determining root causes of incidents, and evaluating the effectiveness of the response process.
4. Identify successes: Determine what went well during the incident response process. This may include successes such as quick response time, effective communication, or successful resolution of the incident.
5. Identify areas for improvement: Identify areas of the incident response process that need improvement. This may include areas such as response time, communication, documentation, or incident management.
6. Develop a plan for improvement: address the identified areas for improvement. This may involve developing new policies or procedures, training for the incident response team, or acquiring new tools or technology.
7. Implement the plan: Put the plan into action and implement the changes to the incident response process.
8. Monitor and evaluate: Monitor the incident response process and evaluate the effectiveness of the changes made. Make further adjustments if necessary.