Rafael Cervantes

01/08/2025

Incident Response Plan

Incident Response Plan (IRP) is a document with guidelines created by an organization to help identify, respond, manage and recover from a cybersecurity incident. Once an incident is detected the organization will need to follow the Incident Response Plan (IRP) to control the situation, if an organization does not have an Incident response Plan (IRP) that could create more damage, like damage reputation, financial loss and longer recovery time. The scope of an Incident Response Plan (IRP) identifies the coverage of the plan, the incidents it covers and the stakeholders involved in the response process. The incidents it covers are data beaches, natural disasters, phishing, malware, Denial-of-Services (DoS) and Distributed Denial-of-service (DDoS) attacks.

The larger the organization the more likely it will be targeted by threat actors. Data beaches is an incident where unauthorized individuals or entities obtain access to protected data. Natural disasters are destructive events caused by natural forces that disrupt an organization's operations. Phishing is a practice of sending fake emails to vendors, third party services providers or an organization to gather personal information or other kinds of sensitive information. Malware is software created to disrupt, damage or gain access to a computer or devices. Denial-of-Services (DoS) is a cyberattack by sending an excessive amount of traffic causing a network, system or application to become unavailable to legitimate users. Distributed Denial-of-Service (DDoS) is a more

powerful version of Denial-of-Services (DoS), launched from multiple sources that have been compromised.

Protecting data is crucial to any organization. Internal data is meant for internal use. Internal data is secured by limiting the access to only employees, using the authentication and access control. Confidential data is data that could harm the organization if it is corrupted or accessed. Confidential data is frequently backed up in secure storage. Confidential data is only accessed by certain employees. Highly sensitive data is protected by encryption, access control and regular monitoring.

The stakeholders involved are the cybersecurity team, legal department, executive teams, public relations team, media, Chief Information Security Officer (CISO) and third party services providers. The cybersecurity team is responsible for the Incident Response Plan (IRP), training and educating the organization about cyber threats, establishing policies, and incident detection. The legal team's responsibilities are legal compliance, risk mitigation, and liability management. The executive team’s responsibilities are decision making, financial oversight and leadership. The public relations (PR) team is responsible for accessing crisis communication management, media relations, and reputation management. The media responsibilities are to manage public perception, reporting, and crisis management. Third party services providers are responsible for incident detection, analysis, recovery, data protection, root cause analysis and future prevention. The Chief Information Security Officer (CISO) is responsible for overseeing the response during a crisis, coordinating the Incident Response Plan (IRP), and restoring business continuity.

There are four incident categories: low, medium, high and critical. Low level incidents have minimal impact on the business like systems bugs and configuration issues. Once a low level incident is detected, the IT team or cybersecurity handle it. Medium level incidents have a moderate impact on the organization such as compromised user credentials and phishing attacks within limited impact.When a medium level incident is reported this requires the management team and the specialized cybersecurity to be involved. High level incidents have a higher impact in the organization often involving system downtime and data breach. The high level incident requires the Public Relations (PR) team, legal team, executive team, cyber security team, third party service team, the Chief Information security Officer (CISO) and media. Critical level incidents are severe incidents such as Distributed Denial of Service (DDoS) and full system compromise. Once a critical level incident is spotted the organization requires all the teams to assemble as fast as possible.

There are six stages: response process preparation, identification, containment, eradication recovery and lessons learned. The goal of preparation is to have the necessary tools, resources and processes to handle and reduce security incidents. Incident response policies and procedures are developed during the preparation stage. Training, exercises, monitoring and implementing security tools are conducted during the preparation stage. During the identification stage, monitoring, detecting and incident classification are being conducted. The containment stage goal is to limit the incident from spreading or evolving. Once the incident is contained, the team needs to inform the response team and coordinate with the Incident Response Plan (IRP). The Eradication state is to remove the

root case of the incident and eliminate any remaining threats. Ensuring that there is no malicious activity left, eliminating back doors, and checking any compromised devices. The recovery stage is restoring the organization back to normal. Monitoring the system after recovery is ideal. During the lesson learned, the organization reviews and learns as much as they can from it so they can prevent a future incident.

Effective communication and notification are critical during an Incident Response Plan (IRP). Stakeholders, communication channels, internal and external entities are notified once an incident is found. Depending on the classification of the incidents different teams are notified. The higher the classification, the more teams are notified.

Training and testing are essential to ensure that team members and staff are prepared for any kind of incidents. Organizations can have meetings with staff members to train and educate them about the cyberattacks. Frequently training and testing the cybersecurity team is ideal. Tabletop is a roleplaying exercise where participants simulcast an incident to test the Incident Response Plan (IRP). Organization should have created a schedule for training their teams. Some organizations have monthly or bi-monlthly exercices. Each exercise should be targeting a different incident. By having frequent exercises the organization has the opportunity to test the effectiveness of tools and Security Information and Event Management (SIEM) systems. Testing the Public Relations (PR) team and legal team could help improve their readiness for a future incident. Testing can also improve the time it takes the team to stop detected elimination and recover the system. Testing also helps refine communication protocols, policies and procedures.

Key Performance Indicators (KPIs) measure the effectiveness of the incident response process. It measures how fast an incident was detected, how long it took to be restored and how effective was the communication during the drill. Continuous training helps the Incident Response Plan (IRP) to evolve to a better Plan by updating it. Since threats keep evolving, the Incident Response Plan (IRP) should be constantly updated.

Risk Management Plan Structure

Risk Management Plan (RMP) is a document that outlines how an organization will identify, assess, manage and monitor risks. Risk Management Plan helps with developing mitigation strategies, risk identification, risk assessment, communication plan, contingency plans, risk monitoring and control. Risk Management Plan (RMP) helps with decision making comprehending the risks. Risk Management Plan (RMP) helps protect the organization resources by reducing the impact of risks.

The scope of the Risk Management Plan (RMP) defines the boundaries within the plan. The organization scope applies for the whole organization addressing risks across all departments. Project specific scope only addresses the risk of the project timelines, and costs. The Chief Risk Officer (RCO) owns the Risk Management Plan (RMP) ensures the plan is specialized for their organization. Cross functional ownership is the distribution of ownership across departments. An example of cross functional ownership of a Risk Management Plan (RMP) is Human Resources (HR) being responsible for human resources risk and the finance department handles financial risks.

Updating and maintaining the Risk Management Plan (RMP) this can help keep the plan current to the potential risks. Tracking emerging risks helps the Risk Management Plan (RMP) stay current with the new technology and new risks. Ensure that all stakeholders are aware of the updated plan. Risk Mitigation addresses each risk whether to avoidance, mitigation, transfer or acceptance. After an incident, a post-incident review should happen to evaluate the effectiveness of the Risk Management Plan (RMP).

The Risk Management Team (RMT) is made out of multiple people: the Chief Risk Officer (CRO)/Risk Manager (RM), risk analysts, compliance officer, cybersecurity risk manager, legal counsel, financial risk officer, IT risk manager, human resources manager, and other executives. Risk Manager (RM) implements the Risk Management Plan (RMP) assessing risks and mitigation activities. Risk analysts perform quantitative and qualitative analysis and track emerging. Compliance officer ensures legal requirements and monitors compliance risks. Cybersecurity risk managers focus on cybersecurity risks, data breaches, and vulnerabilities. Legal counsel assesses legal risks, ensures compliance with the laws and provides guidance during incidents. Financial risk officer controls risks related to financial operations. IT risk manager focuses on IT and technology related risks. Human resources managers focus on human/personnel related risks.

SWOT Analysis (Strengths, Weakness, Opportunities and Threats) is a framework that evaluates an organization's competitive position, helps with decision making, helps determine risks and planning. Checklists can also help identify potential risks by creating a list of risks related to the organization. Using a risk register can help manage risks in a project or organization. A risk register is a tool that helps identify risks from rare to common and low to high risks. Scenario analysis helps imagine various potential risks, exploring the impacts each risk can cause. Historical data and lessons can help the organization prepare and be ready for a future risk. Historical data and lessons help the organization learn from past risks or other companies' risks. The organization also can learn how other organizations dealt with the risks.

There are three levels of likelihood risk criteria: high, medium and low. High level means it is likely to happen. Medium level means it is possible that a risk could happen and low is that a risk is unlikely to happen. There are three levels of impact: high, medium and low. High level of impact means that the consequences are severe such as financial loss or reputation. Medium level impact means moderate impact on the organization function but it is manageable. Low level impact is minimal impact that will not disrupt operations.

Risk treatment determines how to manage and respond to risk based on the likelihood and impact of the risk. It implements actions that either reduce the probability for the risk, reduce the impact or transfer the risk to another party. Risk acceptance means that the organization is okay with taking the risk without trying to reduce it. Risk acceptance happens when the risk is small. Risk mitigation is taking steps to reduce the risk. Risk mitigation happens when the risk is controllable. Risk transfer is transferring the risk to another party. Risk transferring typically happens through contracts, insurance or outsourcing. Risk avoidance is changing plans to avoid a risk that typically happens when the risk is unacceptable. Risk avoidance happens when the risk could damage the organization or project.

Risk monitoring is an ongoing process of monitoring and identifying risks. Performing metric is establishing Key Risk Indicators (KRIs) to monitor the efficiency of controls. Risk Status Reporting is making sure that all of the stakeholders are informed about the current state of risks of the organization. Risk Register is a living document that

provides the status of new ricks, ricks treatments, and outcomes of risk treatment. It is frequently being updated.

Risk communication is important for risk management. Internal communication focuses on keeping everyone within the organization updated and involved with any new information about risks. Risk awareness and understanding helps the organization make smart decisions. External communication involves sharing risk related information with outside parties. This includes customers, suppliers, and stakeholders. Sharing information can help everyone stay informed on new risks and new ways to manage them.

The Risk Management Plan (RMP) needs to be continuously evolving and adapting. Monitoring and documenting risks helps the organizations learn and predict future risks. Communication is key to staying updated with potential risks. Learning from the past or other organizations on how they dealt with risks is the best way to help the Risk Management Plan (RMP) stay relevant and highly effective.