Cyber security long term internship

Smart Internz

Technology stack: cyber security with IBM QRadar

Project title: mastering threat intelligence: strategies for proactive cyber defense

Team ID : LTVIP2024TMID14858

Team size : 5

Team leader : Reddy hema Latha

Team member : Undurthi Anjali

Register number:SBAP0014858

How to build an incident response plan, with examples, template

With cyberthreats and security incidents growing by the day, every organisation needs a solid incident response plan. Learn how to create one for your company.

Cybersecurity professionals work around the clock to prevent security incidents that could undermine the confidentiality, integrity and availability of their organisations information assets. The stark reality, however, is that security incidents will inevitably occur, regardless of safeguards put in place.

A strong incident response plan -- guidance that dictates what to do in the event of a security incident -- is vital to ensure organisations can recover from an attack or other cybersecurity event and minimise potential disruption to company operations.

What is an incident response plan?

An incident response plan is a set of instructions to detect, respond to and limit the effects of an information security event. Sometimes called an *incident management plan* or *emergency management plan*, an incident response plan provides clear guidelines for responding to several potential scenarios, including data breaches, DoS or DDoS attacks, firewall breaches, malware outbreaks, insider threats, data loss and other security breaches.

Why is having an incident response plan important?

Incident response plans help reduce the effects of security events and, therefore, limit operational, financial and repetitional damage. They also lay out incident definitions, escalation requirements, personnel responsibilities, key steps to follow and people to contact in the event of an incident.

An incident response plan establishes the recommended actions and procedures needed to do the following:

- Recognise and respond to an incident.
- Assess the incident quickly and effectively.

- Notify the appropriate individuals and organisations of the incident.
- Organise a company's response.
- Escalate the company's response efforts based on the severity of the incident.
- Support the business recovery efforts made in the aftermath of the incident.

Benefits of a well-crafted incident response plan include the following:

- **Faster incident response.** A formal plan ensures an organisation uses its risk assessment and response activities to spot early signs of an incident or attack. It also helps organisations follow proper protocols to contain and recover from the event.
- **Early threat mitigation.** A well-organized incident response team with a detailed plan can mitigate the potential effects of unplanned events. An incident response plan can speed up forensic analysis, minimising the duration of a security event and shortening recovery time.
- **Disaster recovery (DR) plan launch prevention.** Quick incident handling could save an organisation from invoking more complex and costly business continuity (BC) and DR plans.
- **Good BC.** Organizations such as the Business Continuity Institute and Disaster Recovery Institute International include incident response planning as a key part of the overall BC management process.
- **Better communication for faster action.**Situations exist where the severity of an incident is beyond the capabilities of an incident response team. In these scenarios, incident response teams relay the information they know to emergency management teams and first responder organizations to try and resolve the incident.
- **Regulatory compliance.** Many regulatory and certification bodies require organizations have an incident response plan. To remain compliant with certain regulations, such as PCI DSS, having an incident response plan is critical.

Incident response steps

Organizations don't need to develop their incident response plans from scratch. Several incident response frameworks have been developed by thought leaders in the field.

The NIST "Computer Security Incident Handling Guide" is widely considered to be the authoritative source for incident response planning efforts. It outlines the following four-step incident response cycle:

1. Preparation.
2. Detection and analysis.
3. Containment, eradication and recovery.

4. Post-incident activity.

The SANS Institute's "Incident Management 101" guide suggests the following six steps:

1. Preparation.
2. Identification.
3. Containment.
4. Eradication.
5. Recovery.
6. Lessons learned.

Working within these and other frameworks can help organizations create policies and procedures that guide their incident response actions.

How to create an incident response plan

A well-designed incident response plan can be the crucial differentiator that enables an organization to quickly contain the damage from an incident and rapidly recover normal business operations.

Companies developing their incident response plans should follow these steps.

Step 1. Create a policy

Develop or update an incident remediation and response policy. This foundational document serves as the basis for all incident handling activities and provides incident responders with the authority needed to make crucial decisions. The policy should be approved by senior executives and should outline high-level priorities for incident response.

Designate a senior leader as the primary authority with responsibility for incident handling. This person might delegate some or all authority to others involved in the incident handling process, but the policy should clearly designate a specific position as having primary responsibility for incident response.

When creating a policy, keep the language high-level and general. The policy should serve as a guiding force for incident response but not dive into granular details. Procedures and playbooks fill out those details. The objective is to develop a long-lasting policy.

Step 2. Form an incident response team and define responsibilities

While a single leader should bear primary responsibility for the incident response process, this person leads a team of experts who carry out the many tasks required to effectively handle a security incident. The size and structure of an organization's incident response team varies based on the nature of the organization and the number of incidents that take place. A large global company, for example, could have different incident response teams that handle specific geographic areas using dedicated personnel. A smaller organization, on the other hand, might use a single centralized team that draws on members from elsewhere in the organization on a part-time basis. Other organizations might choose to outsource some or all their incident response efforts.

Whatever team model is chosen, train team members on their responsibilities at the various stages of incident handling, and conduct regular exercises to ensure they are ready to respond to future incidents.

An incident response plan typically requires the formation of a computer security incident response team (CSIRT), which is responsible for maintaining the incident response plan. CSIRT members must be knowledgeable about the plan and ensure it is regularly tested and approved by senior management. Response teams should include technical staff with platform and application expertise, as well as infrastructure and networking experts, systems administrators and people with a range of security expertise.

On the management side, the team should include an incident coordinator who is adept at choosing team members with different perspectives, agendas and objectives to work toward common goals. Task a team member with handling communication to and from management. This role requires someone skilled at translating technical issues into business terms and vice versa.

Data owners and business process managers throughout the organization should either be part of the CSIRT or work closely with it and provide input into the incident response plan. Representatives from customer-facing parts of the business, such as sales and customer service, should also be part of the CSIRT. Depending on the company's regulatory and compliance obligations, legal and PR teams should also be included.

Step 3. Develop playbooks

Playbooks are the lifeblood of a mature incident response team. While every security incident differs, the reality is that most types of incidents follow standard patterns of activity and would benefit from standardized responses. For example, when an employee's phone is stolen, an organization can follow these standard steps:

1. Issue a remote wipe command to the device.
2. Verify the device was encrypted.
3. File a stolen device report with law enforcement and the service provider.
4. Issue the employee a replacement device.

This sequence of steps forms a basic procedure template for responding to a lost or stolen device -- a playbook for handling device theft. The incident response team, therefore, does not need to figure out what steps to take every time a device is lost or stolen -- it can simply refer to the playbook.

As organizations build out their incident response teams, they should develop a series of playbooks that address their most common incident types.

Step 4. Create a communication plan

Incident response efforts involve a significant level of communication among different groups within an organization, as well as with external stakeholders. An incident response communication plan should address how these groups work together during an active incident and the types of information that should be shared with internal and external responders.

The communication plan must also address the involvement of law enforcement. It should outline who in the organization is authorized to call in law enforcement and when it is appropriate to do so. Involving law enforcement can generate adverse publicity, so organizations should make this decision deliberately.

Step 5. Test the plan

Testing the processes outlined in an incident response plan is important. Don't wait until an incident to find out if the plan works. Run simulations to ensure teams are up to date on the plan and understand their roles and responsibilities in response processes. Testing should include a variety of threat scenarios, including ransomware, DDoS attacks, insider data theft and system misconfigurations.

One frequently used testing approach is discussion-based incident response tabletop exercises. During an exercise, teams talk through the procedures they would apply and issues that might happen during a specific security event. A more in-depth testing approach involves hands-on operational exercises that put functional processes and procedures in the incident response plan through their paces. A combination of these two testing approaches is recommended.

Step 6. Identify lessons learned

Each incident that occurs is a learning opportunity. Incident response plans should require a formal lessons-learned session at the end of every major security incident. These sessions should include all team members who played a role in the response and provide an opportunity to identify security control gaps that contributed to the incident, as well as places where the incident response plan should be adjusted. This enables an organization to reduce the likelihood of future incidents and improve its ability to handle incidents that do occur.

Step 7. Keep testing and updating the plan

After creating the plan, conduct testing regularly as processes and threats evolve. Incident response plans should be reassessed and validated annually, at a minimum. They should also be revised whenever changes occur to the company's IT infrastructure or its business, regulatory or compliance structure.

Incident response plan examples and templates

An incident response plan template can help organizations outline exact instructions that detect, respond to and limit the effects of security incidents.

Click to download our free, editable incident response plan template. It is a useful starting point for developing a plan customized to your company's needs. Review it with various internal departments, such as facilities management, legal, risk management, HR and key operational units. If possible, have local first responder organizations review the plan. Their suggestions could prove valuable and increase the plan's success if put into action.

For additional help, review the following incident response plan examples:

- U.S. Department of Homeland SecurityNational Cyber Incident Response Plan.
- Minnesota Department of AgricultureIncident Response Plan for Agricultural Chemicals.
- Bennett College Emergency Response and Crisis Management Plan.
- University at Buffalo Information Security Incident Response Plan.
- Carnegie Mellon Computer Security Incident Response Plan.

- University of Oklahoma Health Sciences Center PCI DSS Incident Response Plan.

An incident response plan is a set of written instructions that outline your organization's response to data breaches, data leaks, cyber attacks and security incidents.

Incident response planning contains specific directions for specific attack scenarios, avoiding further damages, reducing recovery time and mitigating cybersecurity risk.

Incident response procedures focus on planning for security breaches and how organization's will recover from them.

Without a formal IR plan in place, organizations may not detect attacks or may not know what to do to contain, clean up and prevent attacks when detected.

Remember, techniques like IP attribution aren't always helpful and your organization may not be able to recover stolen data and needs to know what it will do in that event.

Why is Incident Response Planning Important?

Incident response planning is important because it outlines how to minimize the duration and damage of security incidents, identifies stakeholders, streamlines digital forensics, improves recovery time, reduces negative publicity and customer churn.

Even small cybersecurity incidents, like a malware infection, can snowball into bigger problems that ultimately lead to data breaches, data loss and interrupted business operations.

A proper incident response process allows your organization to minimize losses, patch exploitable vulnerabilities, restore affected systems and processes and close the attack vector that was used.

Incident response encompasses preparation for unknown and known cyber threats, reliably identifying root causes of security incidents and post-incident disaster recovery.

It allows organizations to establish best practices for incident handling and develop a communication plan that may involve notifying law enforcement, employees and staff.

Incident response is a crucial component of preventing future incidents and running an organization that processes sensitive data like personally identifiable information (PII), protected health information (PHI) or biometrics.

Every security event can have a short term and long term impact on your organization. According to IBM and the Ponemon Institute the average cost of a data breach in 2022 was $4.35 million.

Beyond the cost, business continuity, customer loyalty and brand protection are massive concerns, especially as organizations increasingly rely on third-party vendors.

While it's impossible to remove all security issues, an effective incident response process can mitigate the largest cybersecurity risks.

Who is Responsible for Incident Response Planning?

Organizations should form a computer security incident response team (CSIRT) who is responsible for analyzing, categorizing and responding to security incidents.

Incident response teams can include:

- **Incident response manager:** oversees and prioritizes actions during detection, containment and recovery of an incident. They may also be required to convey high-severity incidents to the rest of the organization, customers, law enforcement, regulations and the public where applicable.
- **Security analysts:** support and work directly with affect resources, as well as implementing and maintaining technical and operational controls.
- **Threat researchers:** provide threat intelligence and context around security incidents. They may use third-party tools and the Internet to understand current and future threats. Organizations will often outsource this function if the expertise does not exist in-house. If this is your organization, look for tools or services that can automatically monitor for leak credentials, data leaks and third-party and fourth-party vendor security posture.

That said, effective incident response relies on cross-functional incident response team members from all parts of the organization.

Without stakeholders from senior leadership, legal, human resources, IT security and public relations, incident response teams can prove ineffective.

Senior leadership support is particularly necessary to gather necessary resources, funding, staff and time from different teams. This may be a Chief Information Security Officer (CISO) or Chief Information Officer (CIO) at a large organization or even the CEO or a board member at smaller organizations.

Legal counsel can help the organization understand which data breaches must be reported to regulators and customers, as well as advice around liability for third-party vendor data breaches.

Where an incident is from an insider threat, human resources can assist with removal of staff and access credentials.

Finally, public relations are essential to ensure an accurate, consistent and truthful message is communicated to the regulators, media, customers, shareholders and other stakeholders.

What are the Different Types of Security Incidents?

There are many types of security incidents and ways to classify them. This is largely an organizational decision, what is considered critical at one organization may be minor at another. That said, there are a range of common cyber incidents every organization should be aware of and plan for:

- Ransomware and other types of malware
- Man-in-the-middle attacks
- Social engineering like phishing and spear phishing
- Exploits of CVE-listed vulnerabilities
- Corporate espionage
- OPSEC failures
- Data breaches
- Data leaks
- Email spoofing
- Domain hijacking
- Typosquatting
- Denial of service (DoS)

Each of these security incidents is common enough to warrant a formal incident response process and recovery plan. Security analysts need to be aware that even small incidents can open up new attack vectors that lead to larger attacks. This is why real-time threat intelligence is so important.

Another important, often overlooked security incident is those that involve your third-party vendors and their vendors. This is known as third-party risk and fourth-party risk.

Security teams need to understand the impact that vendors can have on their organization's security posture. Even if third-parties aren't conducting critical business activities, they still represent significant vendor risk.

This is because they may have access to sensitive data or property, and your organization may be accountable for their security failures.

Avoiding incidents is as much about vendor risk management as it is about managing your internal information security, data security, network security and information risk management.

Look for vendors with SOC 2 assurance, ask to see their information security policy and develop a vendor management policy that contains a third-party risk management framework that allows your organization to easily perform cybersecurity risk assessments on current and potential vendors.

What Tools are Available for Incident Response Teams?

There are tools and industry standards that can be helpful to incident response teams. Tools can be split into three categories:

1. Prevention
2. Detection
3. Response

For prevention, an organization may employ a security scanner and a data leak detection tool to prevent leaked credentials and other sensitive data being exposed due to poor S3 security or a lack of configuration management.

Detection could be covered by antivirus software, network intrusion detection systems, security incident and event management (SIEM) software or a vulnerability scanner that checks CVE.

A common response tool is remediation workflows where incident response teams can request remediation, track and close third-party attack vectors.

Develop and update a plan

Ensure plans and other supporting documents exist and are updated periodically to remain current. All relevant personnel should have access to the parts of the plan that pertain to their responsibilities and should be alerted when the plan is revised. There should be a feedback loop that is enacted after every significant incident in order to improve the plan continuously.

Acquire and Maintain the Proper Infrastructure and Tools

Have the capabilities to detect and investigate incidents, as well as to collect and preserve evidence. To determine if an attacker is in your environment, it’s critical that you have endpoint security technology that provides total visibility into your endpoints and collects incident data.

Without the right tools, and processes to guide their use, you’ll be ill-equipped to investigate how attackers are accessing your environment, how to mitigate an attacker’s existing access, or how to prevent future access.

Always Improve Skills and Support Training

Ensure the IR team has the appropriate skills and training. This includes exercising the IR plan from time to time. It also includes staffing the IR team, with either in-house staff or through a third-party provider, to accommodate the time away from the job necessary in order to maintain certifications and leverage other educational opportunities.

Possess Up-to-Date Threat Intelligence Capabilities

Threat intelligence capabilities help an organization understand the kinds of threats it should be prepared to respond to. Threat intelligence should integrate seamlessly into endpoint protection and use automated incident investigations to speed breach response. Automation enables a more comprehensive analysis of threats in just minutes, not hours, so an organization can outpace advanced persistent threats (APTs) with smarter responses.

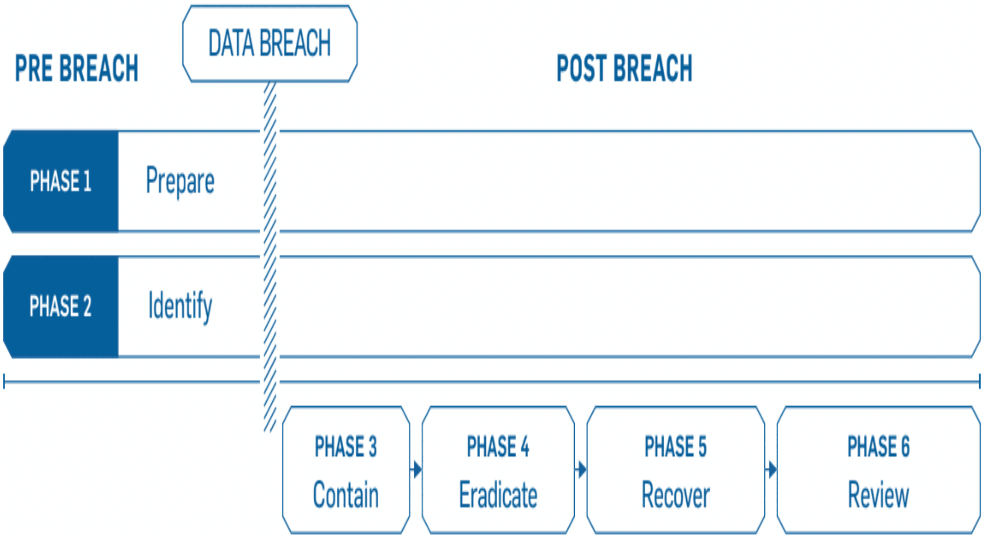
Is an incident response plan a PCI DSS requirement?

Yes, Requirement 12 of the PCI DSS specifies the steps businesses must take relating to their incident response plan, including:

- 12.10.2–Test incident response plan at least annually
- 12.10.3–Assign certain employees to be available 24/7 to deal with incidences
- 12.10.4–Properly and regularly train the staff with incident response responsibilities
- 12.10.5–Set up alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems
- 12.10.6–Implement a process to update and manage the incident response plan per industry and organizational changes

SEE ALSO: What are the 12 requirements of PCI DSS Compliance?

How to create an incident response plan



An incident response plan should be set up to address a suspected data breach in a series of phases. Within each phase, there are specific areas of need that should be considered.

The incident response phases are:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Let's look at each phase in more depth and point out the items that you need to address.

Preparation

This phase will be the work horse of your incident response planning, and in the end, the most crucial phase to protect your business. Part of this phase includes:

- Ensure your employees are properly trained regarding their incident response roles and responsibilities in the event of data breach
- Develop incident response drill scenarios and regularly conduct mock data breaches to evaluate your incident response plan.
- Ensure that all aspects of your incident response plan (training, execution, hardware and software resources, etc.) are approved and funded in advance

Your response plan should be well documented, thoroughly explaining everyone's roles and responsibilities. Then the plan must be tested in order to assure that your employees will perform as they were trained. The more prepared your employees are, the less likely they'll make critical mistakes.

Containment

When a breach is first discovered, your initial instinct may be to securely delete everything so you can just get rid of it. However, that will likely hurt you in the long run since you'll be destroying valuable evidence that you need to determine where the breach started and devise a plan to prevent it from happening again.

Instead, contain the breach so it doesn't spread and cause further damage to your business. If you can, disconnect affected devices from the Internet. Have short-term and long-term containment strategies ready. It's also good to have a redundant system back-up to help restore business operations. That way, any compromised data isn't lost forever.

This is also a good time to update and patch your systems, review your remote access protocols (requiring mandatory multi-factor authentication), change all user and administrative access credentials and harden all passwords.

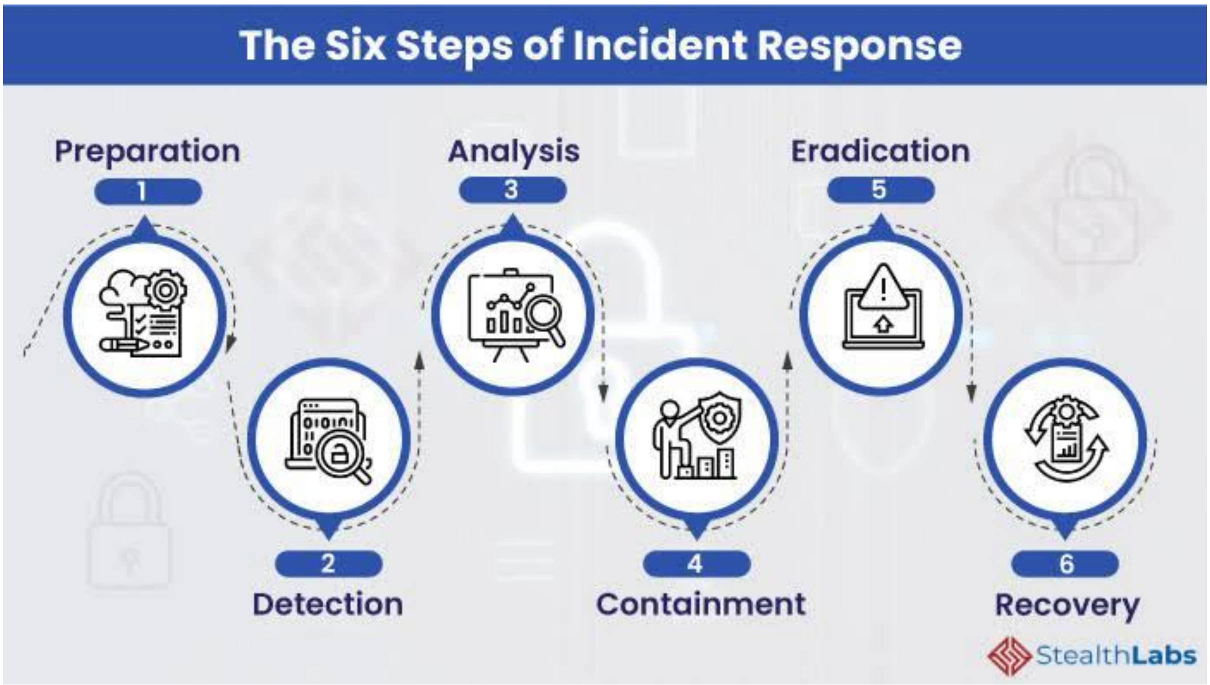
Eradication

Once you've contained the issue, you need to find and eliminate the root cause of the breach. This means all malware should be securely removed, systems should again be hardened and patched, and updates should be applied.

Whether you do this yourself, or hire a third party to do it, you need to be thorough. If any trace of malware or security issues remain in your systems, you may still be losing valuable data, and your liability could increase.

Recovery

This is the process of restoring and returning affected systems and devices back into your business environment. During this time, it's important to get your systems and business operations up and running again without the fear of another breach.



THANK
YOU!