



## Response

### Security Fundamentals

Welcome to Security Lifecycle – Response.

# What you will learn

## At the core of the lesson

You will learn how to:

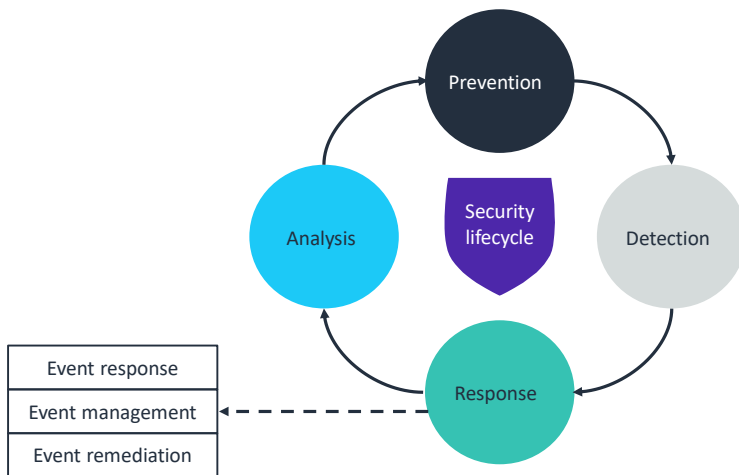
- List the typical steps in the incident investigation process
- Describe the purpose of a business continuity plan (BCP) and a disaster recovery plan (DRP)



In this lesson, you will learn how to:

- List the typical steps in the incident investigation process
- Describe the purpose of a business continuity plan (BCP) and a disaster recovery plan (DRP)

## Security lifecycle: Response



As a review, the phases of the security lifecycle consist of:

- **Prevention** – Is the first line of defense
- **Detection** – Occurs when prevention fails
- **Response** – Describes what you do when you detect a security threat
- **Analysis** – Completes the cycle as you identify lessons learned and implement new measures to prevent the issue from occurring again in the future

In this lesson, you will learn about the *response* phase of the security lifecycle. Specifically, you will discover methods and techniques related to how to manage, respond, and remediate security events.



## Event response analogy

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Next, you'll take a look at an analogy that will bring the idea of event response to life.

## Event response

- Imagine that you're driving on the highway, and suddenly you hear a loud noise. You feel your car start to swerve.
- What would you do next?
  - Pull off the road.
  - Stop the car.
  - Get out and inspect the car.
  - See that you have a flat tire.
  - Notify your employer, family, or friend that you will be late.
  - Replace the flat with a spare tire.
  - Call the garage to fix or replace the tire.
  - Resume your journey by driving carefully and more slowly.
  - After you get a new tire, maybe think about what happened:
    - » Did I pay enough attention to what was on the road?
    - » Was the tire too old?
    - » Should I switch to another brand of tires?



All of these steps represent your response to an incident. They are similar to steps that are used to respond to and investigate a security event.

- What immediate action do you take?
- Whom do you notify?
- How do you ensure that the business can keep running in a reduced capacity?
- How can you ensure that this situation will not happen again or at least that it will be less likely to happen in the future?
- How do you get back to a normal situation?

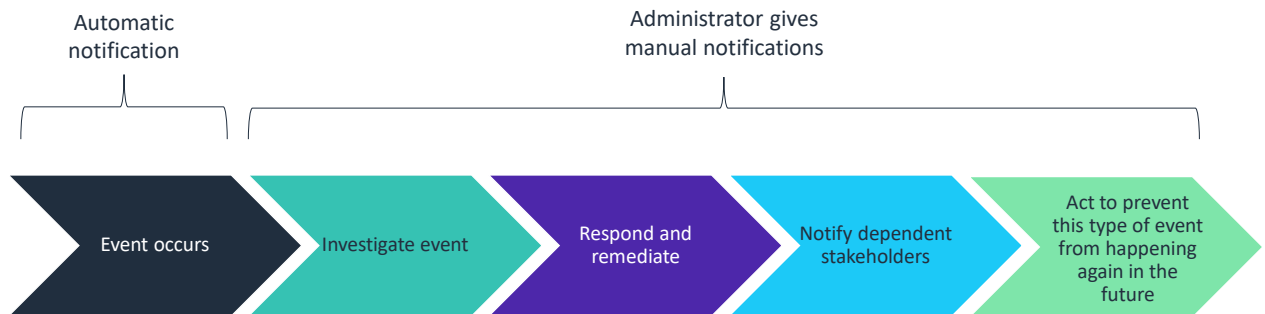
## Process and planning for event response

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Next, you'll define the event investigation process.

# Event investigation process

## Stages of a typical response to any malicious event



The figure shows the typical steps that are used to respond to and investigate a security event.


- When a security alert is activated, the alert must be verified because false positives can happen, especially with a system such as an automated intrusion detection system (IDS).
- If the alert is verified, then the event must be investigated. What is the scope of the attack?
- The first step to respond to the attack is to contain infected elements if there are any, such as hosts infected by a virus. Then, block access to network addresses.
- Notify the departments or the teams that will be affected that they might have limited access to the systems that they use. Stakeholders might be customers that won't be able to use a website.
- Recover to get back to business as soon as possible: add security rules, rebuild infected systems, recover data, and take other appropriate steps.
- Finally, see whether there is a way to strengthen the system to avoid another attack or recover faster. You can also implement new procedures for the team in case of an attack.

You cannot plan for every conceivable disaster. However, you can demonstrate due diligence by identifying and documenting the types of disasters that present a real threat to your business. The unexpected event can be a minor inconvenience, or it

could result in the end of your organization. If you fail to plan for these potential events, you plan to fail.

Tools such as training, systems, and policies can help you prepare for potential events.





## Understanding the business continuity plan (BCP) and disaster recovery plan (DRP)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The next section discusses the business continuity plan (BCP) and disaster recovery plan (DRP).

## BCP and DRP

**A critical aspect of managing a business is creating strategies to prepare for any event that will disrupt the way the business normally works.**

Two strategies or processes are important:

- **BCP:** How to run the business in a reduced capacity
- **DRP:** How to recover from an outage or loss and return to a normal situation as quickly as possible

The purpose of these two plans is to do the following actions:

- Help a business to continue supporting and offering critical services when a disruption occurs.
- Survive a disastrous interruption to activities.

# Planning business continuity

**The BCP is a preventive and proactive management tool.**



- Lists different disaster scenarios
- Lists actions to keep the business running
- Is not activated during an outage

A BCP lists different disaster scenarios. It describes what the business will do to keep critical services and functions running when a disaster or disruption occurs. For example, it could be an interruption of service or destruction of hardware.

The BCP accomplishes the following actions:

- Lists different disaster scenarios and what the business will do to keep business running as usual.

Example scenarios include a failed disk, failed server, failed database, bad communications line, fire, flood, or an earthquake that would make a data center unable to work normally. The disaster could also cause a power outage or require an evacuation of the premises in case of fire. Each of these scenarios could potentially become a security risk.

- Keeps the business running in a reduced form over a period of time.

For example, what is the minimum number of online systems, phones, servers, network connections, network drives, and other resources that must continue to run? Which human resources are affected, and what is necessary to keep the business running? How is security affected, and what priority do secure systems, process, and people have in this scenario?

The BCP is not activated during an outage.

## Planning disaster recovery

**The DRP is a strategy that helps the business recover from disasters and unplanned incidents.**

- **Primary goal:** Restore business functionality quickly and with minimum impact.
- **Security goal:** Do not lower the level of controls or safeguards that are in place.
- **Follow-on goal:** Prevent this threat, exploit, or disaster from happening again.



A DRP defines a strategy that helps the business recover from disasters and unplanned incidents, including cyberincidents. DRP uses two key parameters:

- **Recovery time objective (RTO):** How quickly does the business need to be back up?
- **Recovery point objective (RPO):** How much time and data can the business afford to lose?

As the values of these parameters decrease, backup strategies and other recovery mechanisms become more expensive or complex. However, RTO and RPO have decreased over time as technology has evolved.

The following are possible security goals:

- A business might implement different corrective measures for access control based on the impact of the disaster or disruption. However, the business should implement security access controls to the same level of restriction before the disruption.
- If access controls are not implemented to the same level, the business must not permit access or use of resources.

## Disaster recovery: Understanding recovery time objective (RTO) and recovery point objective (RPO)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

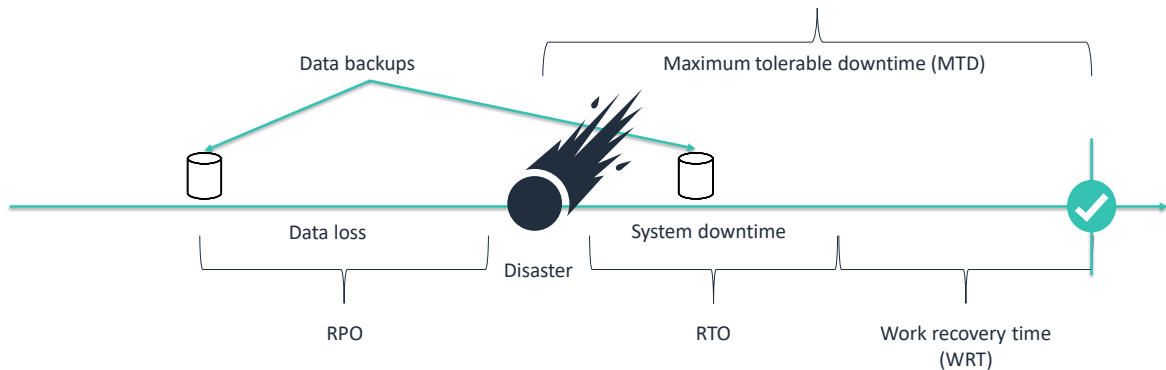
Disaster recovery is the process of preparing for and recovering from a disaster. Examples include earthquakes or floods, technical failures such as power or network loss, and human actions such as inadvertent or unauthorized modifications.

Minimizing the downtime of the systems involves two important objectives:

- **Recovery time objective (RTO):** The maximum acceptable delay between the interruption of service and restoration of service. The RTO determines an acceptable length of time for service downtime.
- **Recovery point objective (RPO):** The maximum acceptable amount of time since the last data recovery point. The RPO is directly linked to how much data will be lost and how much will be retrieved.

## RPO compared to RTO

- **RPO:** How much data can you lose before the business suffers?
- **RTO:** How quickly do you need to recover IT infrastructure to maintain business continuity?



The main focus of RPO is on data. RPO represents the point in time, before disruption, when data can be recovered (given the most recent backup copy of the data) after the disruption. RPO is a factor of how much data loss the business can tolerate during the recovery process.

In short, RPO is concerned with the following questions:

- How much data can the business lose before the business suffers?
- How much time between data backups can elapse without causing severe harm if a disaster occurs?
  - This answer is based on fixed intervals of data backups.
  - The more time that elapses, the more money the business loses.

RPO is easier to implement than RTO because RPO affects only the data layer of your infrastructure.

RTO represents the time that the system can be down before a business can't maintain business continuity and the business suffers.

The sooner a business must get back online, the costlier it will be. Recovery involves the entire business infrastructure.

**Work recovery time (WRT)** involves recovering or restoring data, testing processes, and then making the system live for production. It corresponds to the time between systems and resource recovery, and the start of normal processing.

**The maximum tolerable downtime (MTD)** is the sum of the RTO and the WRT. In other words,  $MTD = RTO + WRT$ .

MTD is the total time that a business can be disrupted after a disaster without causing any unacceptable consequences from a break in business continuity. Include the MTD value as part of the BCP and DRP.



## Disaster recovery options

Recovery from an outage typically relies on the availability of a backup or replication solution that you previously implemented.

- **Backup** (can be traditional tape storage)
- **Replication**
  - Snapshot-based
  - Continuous
- **Pilot light**
  - Minimal version of an environment is always running in the cloud

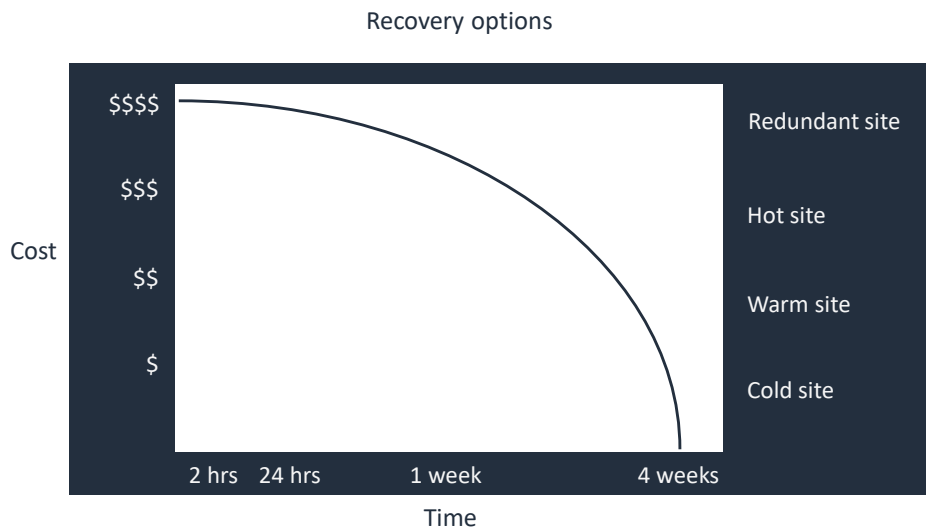
Once you have a deeper understanding of AWS technologies, you can read the AWS whitepaper **Disaster Recovery of Workloads on AWS: Recovery in the Cloud**. This paper provides information that is tailored to cloud services.

The following list contains different types of backup solutions:

- **Backup** (can be traditional tape storage)
  - Is used for the entire business infrastructure
  - Focuses on long-term data of the business
  - Is cost-effective but not time-effective
- **Replication**
  - Snapshot-based:
    - Writes only changed data since the last snapshot
  - Continuous:
    - Uses synchronous, asynchronous, or near-synchronous
    - Focuses on resuming to normal operations quickly
    - Offers more granular recovery points
- **Pilot light**
  - The minimal version of an environment is always running in the cloud.
  - Configure and run the most critical elements of your system.
  - When recovery is needed, rapidly provision a complete production environment around the critical core.
  - Infrastructure elements include database servers and other significant data.

- For AWS related information, see the following resources:
  - Disaster Recovery (DR) Architecture on AWS, Part I: Strategies for Recovery in the Cloud at <https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-i-strategies-for-recovery-in-the-cloud/>
  - Disaster Recovery of Workloads on AWS: Recovery in the Cloud at <https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>

## Cost balancing



15 © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.




The longer a disruption is permitted to continue, the more costly it can be to the business and its operations. A tradeoff exists between speed of recovery and cost.

The answer is not the same for all systems. For example, an employee database can probably be down for a couple of days, but the ecommerce site can be down for only minutes.

Amazon Simple Storage Service (Amazon S3) is a cloud storage service that can back up data with different levels of restoration speed and cost.

For more information about Amazon S3, see the Amazon S3 product webpage at <https://aws.amazon.com/s3/>.



## Activity: Incident response

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Next, you'll learn more about AWS Trusted Advisor through an activity.

## Activity: Objectives

In this activity, you will:

- Identify an incident
- Determine key assets
- Implement an incident response plan
- Specify an eradication solution

### Lab scenario

Your data center has experienced a denial of service (DoS) attack from an unknown attacker. Data network connectivity to the production logistics database is down, and voice communications are being disrupted intermittently. Someone who is taking responsibility for the attack has contacted management and is demanding payment to end the attack.

You are an IT security leader who must interface with the correct internal resources to identify any damage to critical assets.

You are tasked with coordinating measures to stop the attack, identify affected assets, and minimize further damage. You also must recommend controls to prevent this kind of attack from happening again.

In this activity, you will work as a team to document a basic response. Be prepared to suggest and discuss additional information that these documents should capture.

## Activity: Exercise 1

### Identify an incident

The first step of incident response is to determine when the incident occurred. Team members make this determination by completing a short checklist, which might be a series of yes or no questions. If certain answers, or a minimum number of answers, are yes, the team declares an incident, which initiates the incident recovery plan. Based on the scenario for this lab, answer the following questions:

- Has an event occurred that will affect the company?
- Will the event disrupt the confidentiality, availability, or integrity of the company's assets?
- Which type of incident might have occurred (for example, DoS, data loss, equipment, or physical)?
- Is the level of impact low, medium, or high?
- Do you believe that this company is experiencing an incident?
- For the DoS attack described, what groups or managers would be appropriate to contact?

When an incident occurs, it is important to be able to reach needed employees. A good way to do this is to create a form that lists team members and support contacts.

You can get the name, phone, and email of the following persons:

- IT supervisor
- Primary management
- Secondary management
- Facilities management
- Physical security officers or management
- Customer

Most organizations do not have a dedicated incident response team. This list is a sample of appropriate contacts to respond to a particular incident.

## Activity: Exercise 2

### Determine key assets

Placing a value on the key assets of the company is as important as determining whether an incident has occurred. In this exercise, you will determine key assets and assign a qualitative value to each.

- Summarize the initial incident:
  - Note the date, time, location, individual who reported the incident, site point of contact information, and type of incident.
  - For example, note if the incident involved malware, DoS, data loss, equipment failure, malfunction, or power loss.
- Determine how the incident was detected.
- Provide an initial incident description.
- Provide any additional information: IP address, MAC address, server name, system name, and any other information.
- Classify the affected system: mission-critical, sensitive, or departmental.

Collect and note this information to help determine the extent of the problem.

Possible incident types include the following:

- Malware
- DoS
- Data loss
- Equipment failure
- Malfunction
- Power loss

## Activity: Exercise 3

### Implement an incident response plan

#### Incident handler report

- Write down the following information:
  - Individual completing the report
  - Date, contact information, and location of affected systems
  - Time and date of incident response
  - Description of the affected systems

See the next slide for a table to collect information about the affected system.



## Activity: Exercise 3 (continued)

### Implement an incident response plan

Complete the following table:

Affected system	Description	Containment action	Date and time of isolation	Management approved (date and time)	Backup availability
Hardware (manufacturer, model, and version)					
Asset tag # or serial #					
IP address					
Versions					
Other network connectivity information					

21 © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Versions can be the operating system (OS), software, or firmware versions, as appropriate.

Other network connectivity information can be sample virtual local area network (VLAN), switch, and port.

Possible incident containment actions include the following:

- Isolate affected system
- Disconnect from network

Possible options for backup availability include the following:

- Verified
- Secured
- Date and time

## Activity: Exercise 4

### Specify an eradication solution

- Write down the following information about the incident handler report:
  - Individual completing the report
  - Date
  - Manager contact information
  - Root cause analysis details
  - Any additional information
- Create and complete the following table:

Affected system	Eradication solution	Actions to prevent reoccurrence

22 © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Possible eradication solutions include the following:

- Restore from a known good backup
- Reinstall the system
- Replace or repair equipment
- Remove malware
- Repair the facility
- Update the system
- Update the detection system
- Update the prevention system
- Report to human resources (HR)

## Activity: Debrief

### Answer the following questions:

- What are the results of your inquiries?
- Did you discuss new or different issues that the environment is not implementing currently?
- Did you note any legal compliance issues that require a documented incident response plan?

Debrief with your group and the class.

## Checkpoint questions

Which types of plans are used to minimize the impact of unplanned downtime?

What does RTO represent?

Which AWS service can be used to back up data?

1. Which types of plans are used to minimize the impact of unplanned downtime?

Business continuity plan and disaster recovery plan

2. What does RTO represent?

RTO represents the time that the system can be down before a business can't maintain business continuity and the business really suffers. The sooner a business must get back online, the more costly it will be. Recovery involves the entire business infrastructure.

3. Which AWS service be used to back up data?

Amazon S3 is a cloud storage service that can back up data with different levels of restoration speed and cost.

## Key takeaways



- **Planning, investigating, and remediating are key steps** in effectively responding to security events.
- A **business continuity plan (BCP)** and **disaster recovery plan (DRP)** identify and define methods to **prevent an outage** and to **recover as quickly as possible**.
- **AWS offers services, options, and whitepapers** to help implement disaster recovery in a cloud-based environment.

This module includes the following key takeaways:

- Planning, investigating, and remediating are key steps in effectively responding to security events.
- A business continuity plan (BCP) and disaster recovery plan (DRP) identify and define methods to prevent an outage and to recover as quickly as possible.
- AWS offers services, options, and whitepapers to help implement disaster recovery in a cloud-based environment.



# Thank you



© 2022 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections, feedback, or other questions? Contact us at <https://support.aws.amazon.com/#/contacts/aws-training>. All trademarks are the property of their owners.

Thank you for completing this module.