Incident Response Playbook Template

Incident Type

Personal Data Breach

Introduction

This playbook is provided as a template to customers using AWS products and who are building their incident response capability. You should customize this template to suit your particular needs, risks, available tools and work processes.

Security and Compliance is a shared responsibility between you and AWS. AWS is responsible for “Security of the Cloud”, while you are responsible for “Security in the Cloud”. For more information on the shared responsibility model, please review our documentation (https://aws.amazon.com/compliance/shared-responsibility-model/).

You are responsible for making your own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) references current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. This document is provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Summary

This Playbook

This playbook outlines response steps for Personal Data Breach incidents. These steps are based on the NIST Computer Security Incident Handling Guide (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf) (Special Publication 800-61 Revision 2) that can be used to:

- Gather evidence
- Contain and then eradicate the incident
- Recover from the incident
- Conduct post-incident activities, including post-mortem and feedback processes

Interested readers may also refer to the AWS Security Incident Response Guide (https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/welcome.html) which contains additional resources.

Once you have customized this playbook to meet your needs, it is important that you test the playbook (e.g., Game Days) and any automation (functional tests), update as necessary to achieve the desired results, and then publish to your knowledge management system and train all responders.

Note that some of the incident response steps noted in each scenario may incur costs in your AWS account(s) for services used in either preparing for, or responding to incidents. Customizing these scenarios and testing them will help you to determine if additional costs will be incurred. You can use AWS Cost Explorer (https://aws.amazon.com/aws-cost-management/aws-cost-explorer/) and look at costs incurred over a particular time frame (such as when running Game Days) to establish what the possible impact might be.

> ***Warning***
>
> *Besides the procedures outlined in this playbook, your jurisdiction may have requirements and/or legislation about privacy laws (e.g. General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) etc). It may require you to report a security breach and the suspected or confirmed loss or theft of any material or records data. We recommend establishing if this applies to your organization before operationalising this playbook.*

In reviewing this playbook, you will find steps that involve processes that you may not have in place today. Proactively preparing for incidents means you need the right resource configurations, tools and services in place that allow you to respond to an incident.

The next section will provide a summary of this incident type, and then cover the five steps (parts 1 - 5) for handling credential compromise.

This Incident Type

A data breach occurs where there is an unauthorised access to or disclosure of personal information, or information is lost in circumstances where unauthorised access or disclosure is likely that could result in harm or inconvenience, such as fraud or identity theft, to an individual.

What is personal data?

All information that can identify an individual is personal data, directly or indirectly. One example is a person’s name, but also things such as login-ID, birthdate, address, email-address, phone number, social-security number, etc. The concept of personal data goes even further: behavioral or performance data of an individual person (like geo-location, performance-metrics, working hours, device IDs, etc.) are all personal data. The rule of thumb is that if you’re thinking about whether some element could be personal data–it usually is! You should verify whether your systems handle or store personal data. If you have internal teams that can help you with this (legal, policy) check with them. If you do not, you can create and document your own definition based on existing definitions today, such as Article 4 of the GDPR (https://gdpr.eu/article-4-definitions/), or the definition used in various NIST (https://csrc.nist.gov/glossary/term/PII) Special Publications. Commonly, the personal data referred to in this playbook is known as Personally Identifiable Information (PII).

Art. 4 (1) of GDPR (https://gdpr.eu/article-4-definitions/) defines personal data as:

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Incident Response Process

Part 1: Acquire, Preserve, Document Evidence

> ***Note***
>
> *It is important to exercise caution when collecting information during a PII data breach, as personal information must not be recorded. Instead, focus on collecting contextual information surrounding the breach to aid in the investigation.*

1. You become aware that there has been a possible unintended personal data breach. This information could come via different means, for example:

    1. PII was accidentally logged or found in the reporting systems, such as application log files, of your security operations.
    2. An internal ticketing system (the sources of the ticket are varied and could include any of the means below)
    3. A message from a contractor or third-party service provider
    4. From an alert in one of your own monitoring systems, either internal or external, to AWS. For example, in AWS, this might include an AWS Config managed rule, AWS CloudTrail via Amazon EventBridge or Amazon CloudWatch Events and Amazon Simple Notification Service (Amazon SNS), via Amazon Macie, Amazon GuardDuty, AWS Security Hub or a similar service.
    5. From an alert in one of your data loss prevention (DLP) systems
    6. From a threat actor (for example, requesting a ransom or they will disclose data)
    7. From a security researcher
    8. Via an anonymous tip
    9. From a public news article in the press, on a blog, or in the news

2. Confirm a ticket/case has been raised for the incident. If not, manually raise one.

3. Determine the sensitivity of the impacted data and record specific AWS resources that were the origin of the breach. It is also essential to determine the number of individuals who were affected by the incident with certainty (*Contextual information is often a key factors in determining the severity of an incident within an Organization*):

    1. *Nature of personal data:* Your organization's data classification (https://docs.aws.amazon.com/whitepapers/latest/data-classification/data-classification.html) standards

   should also define how to handle a Personal Identifiable Information (PII) data breach. The steps or actions you take may vary depending on the sensitivity/classification of the data involved in the breach, you will refer to your data classification and handling policies to determine this. These standards determine the necessary level of protection for different types of information based on their sensitivity. For example, the level of seriousness for a data breach involving sensitive personal health information of an individual would be greater than that of a breach involving publicly available data:

    1. According to your jurisdiction legal requirements and data classification specifications, it may be necessary to categorize breached data as Personally Identifiable Information (PII) and Publicly Available Information (PAI). Here are few examples:
        - You should consider the breached personal data as PII unless proven otherwise.
        - A common example of PAI is information that is readily accessible to the public, such as a person's name, address, and phone number which is listed in a public directory or on social media platforms.

2. *Number of AWS resources involved:* Below are a few potential scenarios:
    1. An Amazon S3 bucket or an Amazon RDS database was compromised, containing sensitive information such as social security numbers, credit card numbers, banking information, or medical records.
    2. An Amazon Elasticsearch index was lost or compromised, containing personally identifiable information (PII) that should not be publicly accessible.
    3. An Amazon S3 bucket containing personally identifiable information (PII) was compromised and is publicly available. Here are two example scenarios:
        - The bucket was made publicly accessible when it should not have been.
        - The bucket may not have been publicly accessible, but data was still exfiltrated due to credential leakage or an incorrectly configured system that accessed the data and made it publicly available.
3. *Number of individual affected:* This information may help your organization to assess the impact on affected individuals and take appropriate measures to mitigate the consequences, such as offering identity theft protection services or providing timely notifications to prevent further harm.

4. The collection of evidence (AWS CloudTrail logs, AWS Config rules finding etc.) in relation to AWS data services must adhere to a strict chain of custody to ensure the integrity and authenticity of the data as per your jurisdiction legal requirements. Evidence and artifacts can consist of, but aren’t limited to:

    1. All EC2 instance metadata
    2. Amazon EBS disk snapshots
    3. EBS disks streamed to S3
    4. Memory dumps
    5. Memory captured through hibernation on the root EBS volume
    6. CloudTrail logs
    7. AWS Config rule findings
    8. Amazon Route 53 DNS resolver query logs
    9. VPC Flow Logs
    10. AWS Security Hub findings
    11. Elastic Load Balancing access logs

   12. AWS WAF logs
   13. Custom application logs
   14. System logs
   15. Security logs
   16. Any third-party logs

5. At this point, you may not know the cause of data breach:

   1. Extrusion by attackers —an attackers penetrated the security perimeter and,gain access to sensitive personal data.
   2. Insider threats — a malicious insider, or an attacker who has compromised a privileged user accounts, abuses their permissions and attempts to move data outside the organization.
   3. Unintentional or negligent data exposure — an employees who lose sensitive data in public, provide open Internet access to data, or fail to restrict access per organizational policies.

6. If you are already aware of AWS resources involved (like Amazon S3 or Amazon RDS etc) and , Firstly move to **Part 2** to contain the incident. Once that is done, return here and then move on to step 5. If you have not established which bucket(s) are involved, continue to step 4.

7. If you are *not aware* of the AWS resources involved incident personal data breach within an AWS account, follow these steps:

   1. Check AWS services used for data storage and processing, such as Amazon S3, Amazon RDS, Amazon DynamoDB, etc.
   2. Employ the use of internal tools to associate the data with a specific storage location, such as by checking a Configuration Management Database (CMDB).
   3. Review AWS CloudTrail logs for suspicious activity or unauthorized access.
   4. Examine the findings of Amazon GuardDuty in either the source AWS account or the central security monitoring account, focusing specifically on any recent findings, regardless of whether AWS resources are implicated in the incident.
   5. Additionally, review AWS CloudTrail logs to detect any unauthorized access or changes to parameters/secrets in AWS Systems Manager Parameter Store and AWS Secrets Manager. This is important as these services may act as the starting point for managing credentials to access data storage services. To get you started, few examples are:
      1. Analyze Security, Compliance, and Operational Activity Using AWS CloudTrail and Amazon Athena (https://aws.amazon.com/blogs/big-data/aws-cloudtrail-and-amazon-athena-dive-deep-to-analyze-security-compliance-and-operational-activity/)
   6. Please review the access logs for your S3 buckets to identify any unintended or unidentified activity. Here are a few examples of documentation to help you get started:
      1. Logging requests using server access logging (https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerLogs.html)
      2. Identifying access to S3 objects by using CloudTrail (https://docs.aws.amazon.com/AmazonS3/latest/userguide/cloudtrail-request-identification.html#cloudtrail-identification-object-access)
   7. Utilize the *Advanced Queries* feature of AWS Config to analyze any unintentional or unidentified changes to AWS resources and configurations. To get you started, few example queries mentioned here.

    (https://docs.aws.amazon.com/config/latest/developerguide/example-query.html)
    8. Examine Amazon VPC Flow Logs and AWS WAF logs for any anomalous network activity.

8. If you are *aware* of the AWS resources involved:

    1. Consider the following steps to identify suspicious activity or unauthorized access in Amazon S3:
        1. Review Amazon Macie policy findings related to your S3 data (https://docs.aws.amazon.com/macie/latest/user/findings-types.html#findings-policy-types)
        2. Analyze S3 protection in Amazon GuardDuty (https://docs.aws.amazon.com/guardduty/latest/ug/s3-protection.html)
    2. For unintended access to an Amazon S3 bucket refer to this incident response playbook. (https://github.com/aws-samples/aws-incident-response-playbooks/blob/master/playbooks/IRP-DataAccess.md)

9. As previously stated, you maintaining a clear chain of custody is crucial in ensuring the immutability of all evidence. Some of the techniques are mentioned in blog post - Forensic investigation environment strategies in the AWS Cloud (https://aws.amazon.com/blogs/security/forensic-investigation-environment-strategies-in-the-aws-cloud/). In summary, here are the techniques:

    1. Snapshots of Amazon EBS disks: The original EBS disks can be snapshotted, shared to a forensics account, converted into a volume, and mounted in read-only mode for offline analysis.
    2. Manually captured Amazon EBS volumes: Linux tools such as dc3dd can be used to stream the volume to an S3 bucket, along with a hash, and made immutable using an S3 method.
    3. Artifacts stored in an S3 bucket, such as memory dumps: Object Lock in S3 can prevent deletion or overwriting of objects for a specified duration or permanently. MFA delete requires multi-factor authentication to delete an object permanently. Glacier provides a Vault Lock feature to retain evidence in an immutable state over the long term.
    4. Disk volumes: Read-only mode can be used for Linux and write-blocker applications for Windows, some of which are specifically designed for forensic use.
    5. CloudTrail logs: Log file integrity can be validated using CloudTrail's SHA-256 hash and SHA-256 with RSA signing. S3 Object Lock - Governance Mode can be used for protection.
    6. AWS Systems Manager inventory: By default, metadata on managed instances is stored in an S3 bucket and can be secured using the above methods.
    7. AWS Config data: Data stored by AWS Config in an S3 bucket can also be protected through the aforementioned methods.

10. Check if there are any open support tickets for the data storage service, and search for connections with any alerts or information related to the incident. Note any perceived effects on end-users, which may encompass but are not limited to:

    1. Missing data from the storage service
    2. Unexpected presence of new data in the storage service
    3. Changes in access settings (such as permissions) of data, especially if they have been made public
    4. Modified data storage service permissions, access controls, or settings that prevent public access (these may be less noticeable to regular users, but still a possibility)

11. The following are recommendations for internal and external communication regarding a data breach incident, however they may vary based on legal requirements. This example is based on an organization governed by GDPR regulations.

    1. For internal communication, it is important to quickly gather relevant information and assess the scope and impact of the breach. This information should then be shared with the incident response team and relevant stakeholders within the organization. Regular updates should be provided throughout the investigation process to keep everyone informed.
    2. For external communication, it is important to consider the privacy rights of individuals whose PII may have been compromised, as well as the organization's obligations under the GDPR or other relevant legislation/protocols for your jurisdiction. In general, organizations are required to report data breaches to relevant authorities within 72 hours and to notify affected individuals without undue delay.

Part 2: Contain the Incident

Early identification of unusual actions taken by users or strange network activity is crucial in minimizing the harm caused by incidents involving a PII data breach. To prevent the situation from worsening, it's important to take steps to contain the incident, as well as collaborating with your organization's legal and compliance team on any necessary responses and following the incident response plan outlined. Here are a few examples of containment actions for specific AWS services:

1. In this scenario, PII data breach was in an Amazon S3 bucket. Here are the steps you can take to contain the incident:

    1. Identify IAM identities with access to AWS resources
        1. The first step in the process is to identify the IAM identities (which can be either human users or non-human roles) that have access to the AWS resources in question. This is important because it helps to determine the scope of the breach and the extent to which sensitive data has been compromised. Based on this information, you can then take appropriate actions to mitigate the impact of the breach.
    2. Remove access granting policy for the specific IAM role or user
        1. In order to revoke S3 access from an IAM role or user, you need to navigate to the specific S3 bucket where the data breach has occurred. This is where the sensitive data was stored and where unauthorized access occurred.
        2. Once you have navigated to the specific S3 bucket, you need to click on the "Permissions" tab. From there, select the "Bucket Policy" option.
        3. The next step is to remove the access granting policy for the specific IAM role or user. Here is a example policy on how to Managing user access to specific folders. (https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies.html#example-bucket-policies-folders)This will effectively revoke the access of the IAM role or user to the S3 bucket, preventing further unauthorized access to the sensitive data

2. In this scenario, external vendor accounts have been accessing PII stored in DynamoDB tables through SQS and AWS Lambda. The PII data is encrypted using a KMS key at rest and in transit by application, however, due to a defect in the application, some of the PII information may not have been encrypted properly in transit. To contain

this PII data breach, you can take the following actions:

1. Please evaluate the potential business impact of limiting or revoking vendor access to the DynamoDB table, if applicable.
2. If it is acceptable to revoke the access of the vendor, you can do so by updating the access policy to remove their permissions to access the impacted DynamoDB tables and the corresponding SQS queue. This will help to prevent any unauthorized access or use of the resources, which will limit the potential impact of the security breach.
3. Remove the PII data from the logs of the Lambda function that consumes SQS messages. This helps prevent the sensitive information from being further disclosed or compromised. By using Amazon Comprehend and a Lambda function, you can automatically detect and redact PII data in your S3 objects. Following is a tutorial on explaing how this can be accomplished:
    1. Tutorial: Detecting and redacting PII data with S3 Object Lambda and Amazon Comprehend (https://docs.aws.amazon.com/AmazonS3/latest/userguide/tutorial-s3-object-lambda-redact-pii.html)
    2. Sample project to demonstrate how to use AWS SDK for Amazon Comprehend to detect and redact PII data from logs generated by Java applications (https://github.com/aws-samples/comprehend-logging-redact)
4. Conduct a table scan to identify all the rows with unencrypted PII data and update/delete columns.

Part 3: Eradicate the Incident

First step is to determine the affected resources using log data, resources, and automated tooling and then assess each affected resource to determine the business impact of deletion or restoration. Below is an example of eradication steps that can be taken for a personal data exposure that happened due to wide open security group:

1. Identify the potential immediate cause or causes for the PII exposure at hand:

    1. Analyze the collected log data, resources, and tooling to determine the source of the exposure.
    2. Identify if the cause, and then work back through the “5 whys” to get to the root cause https://aws.amazon.com/blogs/mt/why-you-should-develop-a-correction-of-error-coe/ (https://aws.amazon.com/blogs/mt/why-you-should-develop-a-correction-of-error-coe/).

2. It may be helpful to review the infrastructure deployment pipelines, such as those implemented with CloudFormation via AWS Code Pipeline or Terraform, and the data pipelines to determine which mechanism led to the misconfiguration or misclassification of data injection mechanisms. Are there enough checks and balances in the pipeline? If not, it may be necessary to address this issue.

3. If there are any specific issues that have been identified, take steps to remove any resources or configurations that were identified as the immediate causes. For example:

    1. If the cause is a misconfigured security group, adjust the security group rules to prevent unauthorized access.
    2. If the cause is an unauthorized user, revoke their access to the affected resources.
    3. If the cause is a vulnerability, apply patches or upgrades to fix it.
    4. There may be other causes, take the appropriate action.

4. Clean up the environment:

    1. Delete any PII data that may have been exposed.
    2. If PII data must be kept, encrypt it to prevent unauthorized access.

5. Restore normal operations:

    1. Restore permissions and access for authorized users.
    2. Reconnect systems or resources to the network.

Part 4: Recover from the Incident

In addition to restoring the service to a stable and reliable state, it is crucial to inform and provide clear guidance to affected users. Here are the steps you can follow:

1. Coordinate with PR and Legal teams:

    1. Work with your organization's public relations and legal teams to determine the most appropriate approach for communicating with affected users.

2. Update FAQ and Help Center pages:

    1. Utilize your organization's FAQ and Help Center web pages to provide clear and concise information to affected users.
    2. Ensure that the FAQ and Help Center web page are updated regularly with the latest information regarding the incident, including any measures that users can take to safeguard themselves. Here are some sample guidelines that you can provide to your affected external customers in case of identity theft via your application:
        1. *Verify the breach*: Confirm that your personal information has been exposed in the data breach by checking our help centre website.
        2. *Secure your accounts*: Change passwords for any accounts that use the breached information, such as email and financial accounts, and enable two-factor authentication.
        3. *Monitor your accounts*: Regularly monitor your accounts associated with the breached information for any unauthorized activities.
        4. *Place a fraud alert*: Consider placing a fraud alert on your credit report to alert lenders and banks to check with you before opening new accounts.
        5. *Consider credit monitoring:* Consider enrolling in a credit monitoring service to receive alerts about any changes or suspicious activity on your credit report.
        6. *Report the breach*: Report the data breach to relevant government agencies if applicable.
        7. *Stay vigilant*: Be mindful of phishing scams and other attempts to steal your information, and take steps to protect your information going forward.

3. Provide timely information:

    1. Make sure that information is updated in a timely manner to keep affected users informed of the latest developments.
    2. Ensure that the information provided is accurate and easy to understand.

By taking these steps, you can help affected users to stay informed and feel confident that their information and interests are being protected during an incident.

Part 5: Post-Incident Activity

> ***Note***
>
> *It is important to contact legal counsel* ***early*** *to determine if public and individual communication needs to be initiated. Legal counsel can provide guidance on the specific legal requirements and obligations associated with the notification of personal data breaches, including any applicable laws, regulations, and industry standards.*

Once you have removed the affected resources, it's recommended that you perform a security assessment of your AWS account. This assessment can be accomplished by utilizing AWS Config rules, open-source tools like Prowler and ScoutSuite, or other providers. Furthermore, we suggest conducting vulnerability scans on your publicly accessible resources to identify any lingering risks.

In the aftermath of a personal data breach, it is critical to conduct a comprehensive post-incident review to identify areas for improvement and prevent similar incidents from happening in the future. The following post-incident activities can be performed in accordance with the correction of error (COE) concept that is discussed in the following links:

Why you should develop a correction of error (COE) (https://aws.amazon.com/blogs/mt/why-you-should-develop-a-correction-of-error-coe/) Correction of Error (COE) (https://wa.aws.amazon.com/wat.concept.coe.en.html)

1. Review the incident: Perform a thorough review of the incident, including the causes, severity, and impact. This information will be used to determine the effectiveness of the incident response plan and identify areas for improvement.

2. Document lessons learned: Document lessons learned from the incident and use this information to update the incident response plan. This information should include details about the attack vector, the methods used by the attacker, and any other relevant information.

3. Update the incident response plan: Based on the lessons learned, update the incident response plan to reflect any changes or improvements that should be made to the incident response process.

4. Perform a root cause analysis: Conduct a root cause analysis to determine the underlying causes of the incident and to identify any additional areas for improvement.

5. Update policies and procedures: Based on the results of the root cause analysis, update policies and procedures to ensure that the incident response plan is aligned with best practices and regulatory requirements.

6. Implement corrective actions: Implement any necessary corrective actions to prevent similar incidents from happening in the future.