# Microsoft Azure Security Response in the Cloud

Microsoft

## Abstract

## Acknowledgments


# Authors

Ben Ridgway
Frank Simorjay

# Contributors and Reviewers

Alan Ross
Craig Nelson
Monica Martin
Tom Shinder


*Version 1, April 2016*

# Table of Contents

# 1 Introduction

Events such as natural disasters, hardware failures, or service outages are all considered high impact issues, but only a limited number of these issues are considered to be *security incidents*. Microsoft defines a security incident in the Online Services as illegal or unauthorized access that results in the loss, disclosure or alteration of Customer Data.

This white paper examines how Microsoft investigates, manages, and responds to security incidents within Azure. Other service impacting issues that are not security incidents are addressed by a separate response plan (or business continuity plan), and will not be discussed in this paper.

| Non-Security Incident Examples | Security Incident Examples |
|---|---|
| • Routine response to security vulnerabilities that has not resulted in inappropriate disclosure of customer data<br>• A security issue that affects Azure but has not resulted in inappropriate disclosure of customer data<br>• Investigation of internal alarms or monitoring alerts which are shown to be false positives<br>• Operations by Azure's own Red Team activity<br>• Security issues within a customer deployment caused by a flaw or weakness introduced by the customer (failure to patch, brute force, configuration error)<br>• Denial-of-service attack (DoS) against Azure infrastructure or customers<br>• Compliance events that do not affect confidentiality, integrity, or availability of service or customer data | • Unauthorized access to Azure infrastructure systems and exfiltration of customer data<br>• Unauthorized disclosure of sensitive control data, such as credentials, encryption keys, or API keys, which could be used to alter or access customer data<br>• Physical intrusion into a datacenter hosting Azure properties which results in theft of unencrypted customer data<br>• Bug in Azure code which has resulted in malicious alteration or exposure of customer data<br>• Intrusion into a customer deployment caused by a flaw or weakness introduced by the Azure Infrastructure |

*Table 1. Security and non-security incident examples*

This whitepaper is a distillation of the salient points from Microsoft's Security Incident Management procedures for Azure. It provides you with the highlights of how the Azure Security Response team operates during the investigation and response to security incidents.

The goal of security incident management in to identify and remediate threats quickly, investigating thoroughly, and notifying affected parties. Microsoft's process is constantly evolving by tuning out false-positives, automating responses, and contains a framework for evaluating the effectiveness of the program.

Security incident management is an essential part of an effective risk management strategy and critical for compliance efforts. Having a clearly documented processes is crucial because it allows the business to plan ahead for the worst, rather than figuring it out in the heat of the moment. Security incident management is called out by multiple risk and compliance frameworks; for example, ISO/IEC 27035:2011 addresses security incident management.

A holistic security incident response plan enumerates the steps, owners, and timelines for assessing and remediating threats using a repeatable and standardized operating procedure (SOP). Such a procedure ensures that security staff follow a process consistently through manual or automated steps. A security incident response plan is a living document, and it works in concert with other information security management guidelines and standard operating procedures.

The security incident response SOP is designed to be clear and auditable. Responsibilities should map appropriately to roles; individuals who fulfill those roles should have the experience, training, and authority to carry out tasks designated in the plan.

## *1.1 Shared responsibility*

Microsoft uses a shared responsibility model in the Azure services to define security and operational accountabilities. Shared responsibility is particularly important when discussing security of a cloud service because a portion of security responsibility belongs to the cloud services provider while some belongs to the customer.

In a traditional on-premises datacenter, the organization that owns the data center is responsible for managing security incidents end-to-end, including the mitigation and remediation of any security incident.

Conversely, if the same company is using an IaaS offering such as Azure Virtual Machines, security of the physical hosts is the responsibility of Microsoft. The customer tenant can expect to be notified if they were affected by a security incident within the infrastructure hosting that VM. Happenings within the confines of the IaaS VM are outside the service provider's scope, and thus would be a customer responsibility.

Microsoft Azure does not monitor for or respond to security incidents within the customer's area of responsibility. We do provide many tools (such as Azure Security Center) which are used for this purpose. There is also an effort to help make every service as secure as possible by default. That is, it comes with a baseline which is already designed to provide security for most common use cases. This is not a guarantee, however, because there is no way to predict how a service will be used. One must review these security controls to evaluate whether they adequately mitigate risks.

As such, not all security incidents that occur in a cloud environment necessarily involve Microsoft Azure services. A customer-only security compromise would not be processed as an Azure security incident.

A customer-only security compromise would require the customer tenant to manage the compromise response effort and potentially working with Microsoft customer support (with appropriate service contracts).

# 2 Azure Security Incident Response Process

Security incident response is a subset of Microsoft 's overall incident management plan for Azure. The Azure Operations Team is responsible for maintaining the availability of the service. Most events within Azure are not security-related, thus are managed by the Operations team. All Microsoft employees are trained to identify and escalate potential security incidents and escalate appropriately. A dedicated team of security specialists within the Microsoft Security Response Center (MSRC) performs security Incident Response for Azure.

## *2.1 Azure Security Response as it relates to other Microsoft Services*

Microsoft implements a federated security response model. Most major product pillars have dedicated security response teams. This allows deeper specialization into the engineering specifics of their area.

These teams work closely with one another when incidents transcend these product boundaries. The Microsoft Cyber Defense Operations Center is a single location which houses responders from all over the company. It is a way that we can run coordinated incident response as a unified "One Microsoft".

This is important to the scope of this document. For instance, Office 365 and Dynamics CRM have their own dedicated security response team. They are some of Azure's closest partners and are often involved in joint investigations with Azure. The specifies of response outside Microsoft Azure are outside the scope of this document. However, similar processes are often implemented when technology warrants across all Microsoft products and services.

## 2.2 Security Incident Roles and Responsibilities

Microsoft has defined the roles and responsibilities of individuals who take part in the Azure security response process. Predefining roles and responsibilities for individuals involved in an investigation ensures that everyone is aware of their job and prevents inefficiency. Importantly, this also helps provide a capability to manage incidents around the clock. For Azure services, we currently have the following roles and responsibilities identified for security incident response:

| Role | Responsibilities |
|---|---|
| Security Team On-Call | • Initial responder to a suspected security event<br>• Staffed 24x7<br>• Evaluate an incoming event for security-relevance<br>• Escalate to senior security incident manager if necessary |
| Security Incident Manager | • Authority over the response to suspected security events<br>• Works with members of the service team to assess and address the identified issue<br>• Determine if, when, and who to bring in for additional expertise and analysis<br>• Determines whether the event being triaged presents security or privacy risk<br>• Lead the incident team through to closure |
| Security or Forensic Engineer | • Performs disk, log, or memory forensics as needed<br>• Performs in-depth security-related investigation<br>• Preserves evidence as needed is a legal forensically sound manner<br>• Creates finished intelligence reports |
| Communications Manager | • Develops communication content with input from the security incident manager and other experts<br>• Provide notification updates to customers<br>• Provide updates to Microsoft customers and support and service organizations |
| Service Team Experts | • Work with incident response team and incident manager to diagnose and remediate the identified issue<br>• Provides expertise about the operation of their own service should that service be impacted |
| Customer Support Engineer | • Assist with troubleshooting, data collection, and customer communications<br>• Assists with remediation of compromised customer deployments |
| Executive Incident Manager | • Assists the Incident Manager with executive-level decision-making if needed<br>• Assists in communications to customer executives and additional Microsoft executives<br>• Individual with the authority to officially declare a security breach |

*Table 2. Microsoft Azure Security Incident Response roles and responsibilities*

## Security Incident Response Lifecycle

Microsoft follows a 5-step incident response process when managing both security and availability incidents for the Azure services. The goal for both types is to restore normal service security and operations as quickly as possible after an issue is detected and an investigation is started. The response is implemented using a five-stage process illustrated in Figure 3, and described in Table 4, which shows the following activities - Detect, Assess, Diagnose, Stabilize, and Close. The Security Incident Response Team may move back and forth between diagnose to stabilize as the investigation progresses.

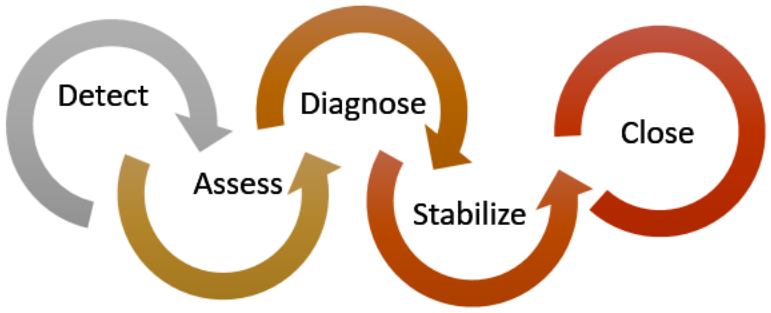


*Figure 1. Incident response activity and states*

| | Stage | Description |
|---|---|---|
| 1 | Detect | First indication of an event investigation |
| 2 | Assess | An on-call incident response team member assesses the impact and severity of the event. Based on evidence, the assessment may or may not result in further escalation to the security response team. |
| 3 | Diagnose | Security response experts conduct the technical or forensic investigation, identify containment, mitigation, and workaround strategies.<br><br>If the security team believes that customer data may have become exposed to an unlawful or unauthorized individual, parallel execution of the Customer Incident Notification process begins in parallel. |
| 4 | Stabilize, Recover | The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps such as quarantining impacted systems may occur immediately and in parallel with diagnosis. Longer term mitigations may be planned which occur after the immediate risk has passed. |

| | | |
|---|---|---|
| 5 | Close/ Post Mortem | The incident response team creates a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence of the event. |

*Table 2. Incident response stages*

### 2.2.1 Stage 1 Detect

Identifying suspicious activity requires a nexus of the latest intelligence capabilities, detection tools, and incident management solutions.

The detection processes used by Azure are designed to discover events that risks the confidentiality, integrity, and availability of Azure services. Several events can trigger an investigation, such as:

- Customer reports via the Customer Support Portal that describe suspicious activity attributed to the Azure infrastructure (as opposed to activity occurring within the customer's scope of responsibility)
- Security vulnerabilities are reported to the Microsoft Security Response Center via secure@microsoft.com. MSRC works with partners and security researchers around the world to help prevent security incidents and to advance Microsoft product security.
- Security Blue and Red teams activity. This strategy uses a highly skilled Red team of experts to attack potential weaknesses in Azure and the security response (Blue team) to uncover the Red team's activity. Both Red and Blue team actions are treated as a means to verify that Azure security response efforts are managing security incidents. Security Red team and Blue team activities are operated under requirements of responsibility to help ensure the protection of Customer Data.
- Detections of suspicious activities by internal monitoring and diagnostic systems within the Azure service. These alerts could come in the way of signature-based alarms such as antimalware, intrusion detection or via algorithms designed to profile expected activity and alert upon anomalies.
- Escalations for operators of Azure Services. Microsoft employees are trained to identify and escalate potential security issues.

### 2.2.2 Stage 2 Assess

The Assess stage of an incident response is a rapid triage effort that includes the following activities:

- Escalating to the Security Response Team's on-call team member (if not already engaged).
- Executing a preliminary assessment and evaluating its details as the investigation continues. The Security Response team's on-call team member will evaluate these preliminary details and determine whether or not security risk exists.
- Assigning the investigation appropriate priority and severity levels. Both the priority and severity maybe changed as the investigation continues, based on new findings and understandings of the investigation. Security events where there is imminent or confirmed risk to customer data are treated as high severity and worked around the clock until resolution.
- Assigning a Security Incident Manager who will be responsible for ensuring that the incident response process is managed through the stages, including tracking cross-dependencies and determining whether it is necessary to include and involve additional service teams that have

been identified at risk in the investigation. The Security Incident Manager role is often assumed by the Security Response Team's on-call team member. However, sometimes a more senior manager will be pulled in to assume this role.

Throughout this process, the Security Incident Manager is ultimately responsible for managing and tracking the investigative process. The Security Incident Manager will ensure that alerts, events, and forensic data generated from multiple sources are investigated and cataloged. They are also responsible for communicating with partner teams to continue the triage process, including the engineering and operations teams to determine whether a given event may affect customers and/or production environments.

### 2.2.3 Stage 3 Diagnose

The goals of the Diagnose stage is to examine the collected information, as well as to gain a better technical understanding of the event. This process may take many resources from many different teams. The Security Incident Manager may bring in additional subject matter expertise to aid in the investigation. An example of this would be bringing in security or forensic analysts to assist.

The Security Incident Manager is expected to:

- Continue to troubleshoot the incident with the help of service teams and additional security personnel.
- Ensure that artifacts are stored in a forensically sound manner.
- Document the investigation with as much technical detail as possible.
- Determine whether customer data is impacted, how, and belonging to which customers.

The information gathered in this stage will be used as the basis of the stabilization and recovery effort (stage 4) if necessary.

This phase may involve forensic examinations of impacted systems. Because investigating forensic images can be sensitive, the ability to do so is tightly controlled and audited. The security response team works closely with global legal advisors to help ensure that forensics are done in accordance with legal obligations and commitments to our customers.

If at any time the investigation is determines that unauthorized or unlawful access resulted in the loss, disclosure, or alteration of any Customer Data, the Security Incident Manager will immediately begin executing on the Customer Incident Notification Process. In the course of the investigation, Microsoft may also determine that other compliance and security risks exist, but do not result in the unauthorized or unlawful access of customer data. In those cases, the security incident manager will continue driving these issues to closure even though the customer incident notification process is not necessarily triggered.

### 2.2.4 Stage 4 Stabilize and Recover

The Stabilize and Recover stage consists of a process designed to correct and repair services affected by a security event. The process is tracked and tested to help ensure that corrective measures are applied effectively to maintain operational success. The goals of this stage is to:

- If necessary, take emergency mitigation steps to resolve immediate security risks associated with the event.
- Verify that customer and business risk has been successfully contained, and that corrective measures are being implemented.
- Identify additional mitigation and corrective measures and long-term solutions if needed.

Mitigation action

During the Diagnose and Stabilize stages, it may be possible that the response team identifies an emergency mitigation or containment step to minimize the impact of an event. The executive incident manager, service owner, and security incident manager may jointly choose to take immediate emergency mitigation steps when needed. For instance, it is possible that these actions may result in a temporary outage. Such decisions are not taken lightly. When such an aggressive mitigation occurs, the standard processes for notifying customers of outages and recovery timelines would apply.

### 2.2.5 Stage 5 Close and Post Mortem

After a security incident, Microsoft will complete an internal post-mortem on the event to address:

- Technical or communications lapses, procedural failures, manual errors, process flaws that might have caused the security incident or that were identified with a post mortem are identified.
- Identified technical lapses that are captured and can be followed up on with engineering teams.
- Response procedures that are evaluated for sufficiency and completeness of operating procedures.
- Updates that may be necessary to the Security Incident Response SOP or any related security response processes.

Internal postmortems for security events are highly confidential records which are not available to customers. They may, however, be summarized and included in other customer event notifications. These reports are provided to external auditors for review as part of Azure's routine audit cycle.

The incident manager is accountable for drafting the post mortem report and maintaining an inventory of all repair items, their owners, and completion dates.

## *2.3 Customer Security Incident Notification*

If during the investigation of a security event, Microsoft becomes aware that customer data has been accessed by an unlawful or unauthorized party, the security incident manager will immediately begin execution of the Customer Security Incident Notification Process. This can occur at any point of the incident lifecycle, but usually begins during the Assess or Diagnose phases. The security incident manager only needs reasonable suspicion that a reportable event has occurred to begin execution of this process. The investigation and mitigation need not be completed before this process begins in parallel.

The goal of the customer security incident notification process is to provide impacted customers with accurate, actionable, and timely notice when their customer data has been breached. Such notices may also be required to meet specific legal requirements.

### 2.3.1 Determine Scope of Impacted Customers

Microsoft relies on heavy internal compartmentalization in the operation of Azure. Logs about whose data was where and when are also robust. Due to these factors, most incidents can be scoped to specific customers. The goal is to provide anybody who is impacted as detailed a notice as possible.

### 2.3.2 Notice Creation

The goal of this notice is to provide customers with detailed enough information so that they can perform an investigation on their end and meet any commitments they have made to their end users while not unduly delaying the notification process. A notice has no value if it provides limited information. It is also very time sensitive. The incident notification team must balance speed with completeness bounded by applicable legal and contractual obligations.

Generally, the process of drafting notifications occurs as the incident investigation is ongoing. The security response team will move quickly and accurately. Additional experts in security communications and legal are often brought in to assist with this process.

### 2.3.3 Confirmation and Incident Declaration

As the incident investigation progresses, the security response team will amass evidence showing whether or not a breach has occurred. This evidence is presented to the designated executive who reviews it with the advice and expertise of the entire team. If a draft notice is ready, that too will be reviewed for accuracy and completeness.

If the designated executive is satisfied that unauthorized access or a security incident has occurred, an incident declaration will occur. This declaration triggers the process of sending official notifications.

### 2.3.4 Customer Incident Notification

When a security incident is declared, Microsoft supports an incident notification process for Azure that includes:

- Prompt notification to affected customers
- In some instances, notification may be delayed at the direction of law enforcement, in which case Microsoft will endeavor to take precautions for the mitigation of the issue and minimize impact to our customers
- Notification to applicable regulatory authorities if required

Notification of security incidents will be delivered to the listed security contacts provided in Azure Security center, which can be configured by following the implementation guidelines. Additionally, if contact information is not provided in Security Center, notification will be sent to one or more of a customer's administrators. Notification will be sent by any means Microsoft selects, including via email. Email is considered the most desirable approach for most issues. It provides the security response team great bandwidth to notify a lot of customers quickly.

To ensure that notification can be successfully delivered, the customer is responsible for ensuring that the security contact, and administrative contact information on each of their subscription(s) and online

services portal(s) is correct. Emails may also be distributed to the subscription co-administrators of the impacted subscription(s).

### 2.3.5 Notification Timeline

In the event of a declared security incident, notification by Microsoft will be made without unreasonable delay and in accordance with any legal or contractual commitments. Customers should recognize that an exercise balancing between accuracy/completeness and speed takes place.

### 2.3.6 Additional Notification

Microsoft may choose to notify our customers of issues even when the issue is not a security incident. This generally occurs when we perceive a widespread risk to our customer base that is unusual in nature. Examples include requesting specific action of customers to address such issues as application security or unpatched vulnerabilities, applying new settings, or investigating logs for a specific issue. Microsoft's obligation to provide notification about issues within a customer's scope of responsibility is not an acknowledgement by Microsoft of any fault or liability with respect to that security issue.

## Team readiness and training

Microsoft personnel are required to complete security and awareness training, which helps them to identify and report suspected security issues. Operators working on the Microsoft Azure service have addition training obligations surrounding their access to sensitive systems hosting customer data.

Microsoft security response personnel receive specialized training for their roles. There are numerous training curriculums offered commercially to prepare security response and forensics personnel for their duties. The MSRC Azure Security Response team uses an additional apprenticeship period to train new Security Incident Managers. It is only after a long period of working with a senior member of the team that a new member in considered ready to run a security event.

Multiple times throughout the year, Azure performs tests of the incident response capability. Some of these occur in response to operations by the Azure Red Team. The Azure Red Team is continuously testing the security posture of the Azure Infrastructure. When detected, the Security Response team (also known in this case as the Blue Team) acts as if the adversary was real in all ways. The only difference between the Red Team and an outside adversary is that the Red Team is prohibited from actually accessing customer data, such that the Red Team should not create an actual security incident.

In addition, Microsoft periodically conducts cross-company Red Team versus Blue Team exercises. These exercises extend across multiple Microsoft services. They ensure that all security responders are able to act as one cohesive unit when an incident transcends one product line.

The security response team devotes significant resources to preparing for incidents before they occur. Besides the aforementioned exercises, Azure security response has a significant development team who creates tooling and procedures in response to prior or anticipated incidents. Tabletop exercises also occur particularly with new features to help them think through scenarios during their design and development phases. That way they are prepared, should the worst happen.

## Conclusion

The security incident management program is a critical responsibility for Microsoft, and represents an investment that customers using Microsoft Online Services can count on. The five-stage process presented in this white paper is a process that has evolved over many years – and continues to do so – and involves a team of dedicated experts with skill and dedication to protecting Microsoft customers.