Version: 1.0

Business continuity, disaster recovery, and crisis management at Twilio

Contents

Introduction

Organizations of all sizes and industries rely on Twilio's cloud communications platform to power millions of customer engagement experiences every single day. We understand that the reliability of Twilio's platform, products, and people is essential to helping organizations build connections and trust with their customers, partners, and employees at scale. We take measures to protect our customers and their services through our high-availability platform architecture, resiliency practices, and requirements built into our development and operational processes and by maintaining Business Continuity, Disaster Recovery, and Crisis Management programs to mitigate risks and safeguard our people, customers, business, and products.

This document provides an overview of Twilio's Business Continuity, Disaster Recovery, and Crisis Management programs.

The resilience programs

Twilio's Business Continuity, Disaster Recovery, and Crisis Management programs are committed to providing solutions and strategies that protect Twilio's top priorities: our people, products, and customers. Our framework aligns with ISO 22301 Business Continuity Management Systems and the Business Continuity Institutes' Good Practice Guidelines.

The resilience programs were progressively established in late 2018 and early 2019. Today, they cover Twilio customer-facing products and services and the critical internal processes and teams supporting the delivery of these products and services. The programs collectively enable Twilio to provide and maintain controls and capabilities for managing Twilio's overall ability to continue to operate during disruptions.

Twilio's team

Twilio has dedicated Business Continuity, Disaster Recovery, and Crisis Management teams composed of experienced industry experts who have designed and implemented custom programs for organizations of comparable size and industry to Twilio, with a focus on deep subject matter expertise in regulatory compliance frameworks and cloud service architecture.

Guiding principles

Safeguard our people
Our community of Twilions is the most important asset to Twilio. We make the well-being of our people a top priority by providing a safe and secure working environment. If needed, support and response are implemented to account for and ensure the safety of our people.

Protect the business
In addition to focusing on our people, our proactive approach to planning focuses on processes, technology, and third parties to avoid downtime and reduce the impact of adverse events.

Manage risk
Twilio's resilience programs help identify and understand risk across the business, resulting in greater consistency and traceability of our products and services. This means problems are easier to avoid and manage once they happen.

Foster customer trust
We pride ourselves on being the most trusted and reliable engagement platform. Embedding resilience practices into our operations enables us to deliver dependable products and services that consistently meet customer requirements.

Follow best practices
We acknowledge and understand that statutory and regulatory requirements impact both Twilio and our customers. We work thoughtfully to incorporate industry best practices, such as ISO/IEC 27001, in our resilience practices.

Twilio's process

Twilio uses a top-down approach to set the scope of our resilience programs. That means we start with the products and services we offer and work backward to include the teams, functions, and resources that support their delivery. Our programs encompass not only the engineering teams that directly support the delivery of Twilio's products but also the many back-office teams and functions that enable Twilio in less direct but equally important ways.

Business continuity

Business Continuity is the capability of the business to continue the delivery of products and services at acceptable, predefined levels following a business disruption. Twilio's business continuity program follows an annual program cadence of core activities ranging from business impact analysis, plan development and updates, and testing/exercises.

Business impact analysis

Twilio performs an annual business impact analysis (BIA) to understand business requirements, set recovery objectives, and identify gaps and areas of vulnerability. The requirements and objectives established during the BIA inform the strategy analysis and planning processes. Risks identified during the BIA are included in the enterprise risk management processes. BIAs are reviewed, updated, and approved annually by leadership or as significant organizational changes occur.

Strategy analysis

Following the BIA, Twilio's resilience team works with business unit leadership and functional owners to identify current-state strategies for recovery should a disruptive event occur. Twilio uses a resource-based planning approach and focuses on documenting realistic, current-state strategy in the event of a loss of a key resource such as an application, technology system, facility, third-party software or equipment, personnel, or any other key enabler of critical functions.

Business continuity planning

With strategies defined, Business Continuity Plans (BCPs) are updated to specify how teams will respond and recover during a disruptive event. BCPs are in place for each in-scope team, and teams have ownership of their plans–validating that the plan content is usable, actionable, and accurate. Plans are reviewed, updated, and approved annually by leadership or as significant organizational changes occur.

Third-party assurance

Twilio evaluates the business continuity capabilities of key vendors and third parties through a third-party security assessment embedded in the procurement process.

Disaster recovery

Disaster Recovery is the ability of the information and communication technology elements of an organization to support its critical business functions to an acceptable level within a predetermined time following a disruption. This is achieved through a framework of activities based on policy, the service readiness framework, site reliability engineering, incident command, and compliance requirements.

Twilio's infrastructure for Twilio, Segment, and SendGrid services uses various tools and mechanisms to achieve high availability and resiliency. For Twilio Services, Twilio's infrastructure spans multiple fault-independent AWS availability zones in geographic regions physically separated from one another. For Twilio Services, there are manual or automatic capabilities to re-route and regenerate hosts within Twilio's infrastructure. Twilio's infrastructure can detect and route around issues experienced by hosts or even whole data centers in real time and employ orchestration tooling that can regenerate hosts, building them from the latest backup.

Twilio leverages specialized tools that monitor server performance, data, and traffic load capacity within each availability zone and co-located data centers. If suboptimal server performance or overloaded capacity is detected on a server within an availability zone or co-located data

center, these specialized tools will increase the capacity or shift traffic to relieve any suboptimal server performance or capacity overload. Twilio will be notified immediately and have the ability to take prompt action to correct the cause(s) behind these issues if the specialized tools are unable to do so.

This methodology allows automatic failover of nodes from primary to backup should the primary fail for any reason, be it physical or logical. Should automatic failover not happen, the company's incident command process is invoked to manually recover and inform the Crisis Management team, if needed.

Twilio performs regular backups of customer data, which is hosted on AWS's data center infrastructure. Customer data that is backed up is retained redundantly across multiple availability zones and encrypted in transit and at rest using the Advanced Encryption Standard.

Testing

Plans are tested as part of the annual implementation of the program lifecycle via procedural walkthroughs, tabletop exercises, and simulations. Test scenarios are based on likely threats to the business as identified via risk management functions and vary in complexity as related to the objectives of the exercise (e.g., regional outage, people loss). Lessons learned and betterments are identified and documented as part of the exercise and reported and tracked to completion.

Twilio's Recovery Time Objectives (RTOs) are set based on possible impacts from a disruption, enabling and protecting Twilio's customer-facing SLAs. While Twilio doesn't provide RTOs for review, time frames are designed to ensure Twilio can meet obligations, both internally and externally. Customers can subscribe to real-time status updates for Twilio products at status.twilio.com/.

Crisis management

The mission of Crisis Management at Twilio is to prepare for and lead Twilio's response to enterprise-level incidents while preserving the health and well-being of our employees, the integrity of business operations, and public & customer trust in the company. Twilio accomplishes this by preparing for, responding to, and recovering from a wide range of high-impact adverse events, such as a major cybersecurity event, severe product failures, or safety and security issues affecting a large portion of Twilions.

Twilio defines a crisis as a unique set of circumstances that disrupts normal business operations and requires swift, coordinated, or higher authority decision-making to mitigate significant or imminent risk to the business. The event may severely jeopardize the company's people, technology, reputation, operations, or finances.

The Crisis Management team takes a coordinated, enterprise-wide approach to each crisis with a dedicated core response team and an extended team that provides subject matter expertise and solutions. Dedicated program managers oversee the program and provide the management structure and processes to enable a coordinated and effective response.

Crisis management plan

A corporate crisis management plan is in place to govern a global response following an incident impacting Twilio. The plan includes the assembly of a core team of leaders and procedures for decision-making and communications.

Criteria

Twilio has established criteria (triggers and thresholds) across the business for managing incidents and escalations. These criteria are based on the impacts to the enterprise and our products & services as well as customers. These criteria inform the processes for activating plans, assembling recovery teams, and making critical decisions.

Summary

Business Continuity, Disaster Recovery, and Crisis Management are integral programs at Twilio in maintaining the standard of service customers have come to expect. As we continue to grow and expand our product offerings, resilience is a continuous effort and our investment in these programs reflects our commitment to safeguarding our people, customers, their data and the products and services we provide.

For more information about business continuity at Twilio, reach out to your Account Executive or visit twilio.com/help/sales.

Key points

- Business Continuity, Disaster Recovery, and Crisis Management safeguard Twilio's people and business during adverse events
- Program mission statements:
  - Business Continuity: Continue the delivery of products and services at acceptable levels during adverse events
  - Disaster Recovery: Ensure recovery of technology elements of the business following a disruption
  - Crisis Management: Avert potential crisis events and manage those that occur
- The core objectives are to maintain product availability while protecting our people and technology during disruptive events
- The programs follow an annual cadence of preparing for, providing, and maintaining controls and capabilities for managing Twilio's overall ability to continue to operate during disruptions
- Twilio's approach to resilience is aligned to ISO 22301 Business Continuity Management System and the Business Continuity Institutes' Good Practice Guidelines