hackerone

REPORT ON HACKERONE INC.'S BUG BOUNTY & VULNERABILITY DISCLOSURE PLATFORM RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY THROUGHOUT THE PERIOD JULY 1, 2019 TO JUNE 30, 2020

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

COALFIRE CONTROLS

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: HackerOne Inc. ("HackerOne")

SCOPE

We have examined HackerOne's accompanying assertion titled "Assertion of HackerOne Inc. Management" (assertion) that the controls within HackerOne's Bug Bounty & Vulnerability Disclosure Platform (system) were effective throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that HackerOne's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

SERVICE ORGANIZATION'S RESPONSIBILITIES

HackerOne is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that HackerOne's service commitments and system requirements were achieved. HackerOne has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, HackerOne is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

SERVICE AUDITOR'S RESPONSIBILITIES

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve HackerOne's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve HackerOne's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

INHERENT LIMITATIONS

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

OPINION

In our opinion, management's assertion that the controls within HackerOne's Bug Bounty & Vulnerability Disclosure Platform were effective throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that HackerOne's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

RESTRICTED USE

Certain complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HackerOne, to achieve HackerOne's service commitments and system requirements based on the applicable trust services criteria. Users of this report should have sufficient knowledge and understanding of complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements. HackerOne uses Amazon Web Services (AWS) as a data center colocation provider. Users of this report should obtain the relevant AWS SOC 2 or SOC 3 reports.

Coalfire Controls LLC

Westminster, Colorado
September 10, 2020

SECTION 2

ASSERTION OF HACKERONE INC. MANAGEMENT

hackerone

Assertion of HackerOne Inc. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within HackerOne Inc.'s ("HackerOne") Bug Bounty & Vulnerability Disclosure Platform (system) throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that HackerOne's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that HackerOne's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). HackerOne's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that HackerOne's service commitments and system requirements were achieved based on the applicable trust services criteria.

HackerOne Inc.

ATTACHMENT A

HACKERONE INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS BUG BOUNTY & VULNERABILITY DISCLOSURE PLATFORM

TYPE OF SERVICES PROVIDED

HackerOne Inc. (or “the Company”) is a provider of bug bounty and vulnerability coordination solutions, helping organizations find and fix critical vulnerabilities before they can be exploited. The Company is headquartered in San Francisco with offices in London, New York, Paris, the Netherlands, and Singapore.

BUG BOUNTY & VULNERABILITY DISCLOSURE PLATFORM

The Bug Bounty & Vulnerability Disclosure Platform (“HackerOne Platform”) enables crowdsourced vulnerability discovery and disclosure activities. This is done by giving customers access to a large and diverse number of crowdsourced security researchers (also called finders or hackers). This enables researchers to conduct remote, internet-based, crowdsourced vulnerability discovery and disclosure services against internet-accessible assets, including public-facing and private-facing websites, networks, systems, and applications.

The HackerOne Platform facilitates communication between the customer, triage personnel, and security researchers through the creation of customized vulnerability management workflow to track vulnerabilities throughout the remediation lifecycle. In addition, the coordination of vulnerability disclosures that impact third-party organizations or vendors is managed within the HackerOne Platform to maintain secure transmission and storage throughout the disclosure lifecycle.

HELPDESK AND SUPPORT

The Company provides customer support for its HackerOne Platform through a dedicated Support Team via email at support@hackerone.com. A documentation center (https://docs.hackerone.com/) is provided, and a support ticketing system is maintained.

The boundaries of the system in this section of the report details the HackerOne Platform. Any other Company services are not included within the scope of this report.

THE BOUNDARIES OF THE SYSTEM USED TO PROVIDE THE SERVICES

The boundaries of the HackerOne Platform are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the HackerOne Platform.

The components that directly support the services provided to customers are described in the subsections below.

INFRASTRUCTURE

Because the HackerOne Platform operates as a software-as-a-Service (SaaS) solution hosted in a public cloud, the Company does not have significant hardware aspects for its own infrastructure. The Company’s production infrastructure is entirely hosted in Amazon Web Services (AWS). AWS operates under a shared responsibility model. Under this model, “AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.” The Company leverages the experience and resources of AWS to enable the Company to quickly and securely scale as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the HackerOne Platform architecture

within AWS to ensure the availability, security, and resiliency requirements are met. The AWS services used by the HackerOne Platform are hosted primarily in the AWS US East/West regions us-west-2 (Oregon), us-east-1 (Virginia), and us-east-2 (Ohio). Additional services as part of the Company's Gateway add-on are hosted in the AWS region ap-south-1 (Mumbai, India) with all data storage occurring in the aforementioned AWS US East-West regions.

The Company deploys virtualized infrastructure into Amazon Virtual Private Clouds (Amazon VPCs) that are segmented and isolated by role within its development and production workflow. This design prevents direct network connections between production, staging, testing, and corporate resources. The Terraform policy that defines these VPCs and network rules is checked into source control and any changes are peer reviewed before deployment.

The in-scope hosted infrastructure also consists of multiple supporting tools as shown in the table below:

Infrastructure			
Production Tool	**Business Function**	**System Software**	**Hosted Location**
Data Stores	Customer data storage	PostgreSQL, Redis, DynamoDB, Snowflake	AWS
Operating System	Virtualized infrastructure	Ubuntu Linux LTS	AWS

SOFTWARE

The Company deploys a mix of open source software and managed SaaS products.

The HackerOne Platform is an internet-facing web application built on the Ruby on Rails framework available to the Internet. Requests to the HackerOne Platform flow first through Cloudflare, a third-party application that provides Domain Name System (DNS) and Layer 7 distributed denial-of-service (DDoS) protection on the Company's behalf. Cloudflare then passes traffic on to a stack that is operated by the Company, with Layer 7 HTTPS security on an AWS Application Load Balancer (ALB).

AWS ALBs route traffic and load balance between HackerOne Platform frontend application instances served by Amazon Elastic Compute Cloud (Amazon EC2), which run Nginx, Unicorn, and Rails. These frontload application instances service requests for the Company's customers, security researchers, and API traffic.

Application instances use a variety of backend services to fulfill requests, including:

Software	
Production Application	**Business Function**
PostgreSQL (via Amazon Relational Database Service [Amazon RDS])	Relational database
Redis (via Amazon ElastiCache)	Caching
Amazon DynamoDB	Key/Value store

Software	
Sidekiq, Shoryuken (via Amazon Simple Queue Service [Amazon SQS])	Queuing and asynchronous processing
Amazon VPC	Private cloud
AWS CloudTrail, AWS Config	Activity monitoring and auditing
Amazon Route 53	DNS
Amazon Simple Email Service (Amazon SES)	Email delivery
Amazon Simple Notification Service (Amazon SNS)	Publish/subscribe messaging
Amazon Simple Storage Service (Amazon S3), Amazon S3 Glacier	Object storage and logging
Amazon Inspector, AWS Security Hub	Vulnerability management
Amazon GuardDuty	Intrusion detection
osquery	Endpoint visibility, file integrity monitoring, process auditing, baseline compliance, intrusion detection, vulnerability management, and malware detection
Fluentd, Amazon Kinesis Data Firehose, Amazon Kinesis Data Streams, Amazon CloudWatch Logs	Logging
Terraform, AWS CloudFormation	Configuration management (infrastructure)
Ansible	Configuration management (Linux)
AWS Identity and Access Management (AWS IAM)	Identity and access management
AWS Key Management Service (AWS KMS)	Key management
AWS Lambda	Serverless infrastructure
Vault	Secrets management
Git	Source control management
GitLab	Development collaboration, code review, task management, continuous integration, and deployment
Sumo Logic	Log analysis and monitoring and anomaly detection
PagerDuty	On-call rotation, escalation, and incident tracking
Pingdom	Edge monitoring and uptime statistics

Software	
Snowflake	Data warehouse
Fivetran	Data pipeline
Amazon CloudFront	Content delivery network
AWS Shield	DDoS prevention
Cloudflare	Content delivery network, DDoS prevention, and DNS
Amazon CloudWatch, Datadog, New Relic	Metrics and performance monitoring
Google Analytics, Mode	Analytics
Slack	Collaboration and communication
StatusPage	Customer incident and uptime communication
Twilio	Short message service (SMS) notification
Zapier	Workflow automation
Zendesk	Helpdesk and ticketing system

PEOPLE

The Company develops, manages, and secures the HackerOne Platform via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	• Responsible for overseeing Company-wide activities, establishing and accomplishing goals, and overseeing objectives.
Employee Success (Human Resources [HR]) Department	• Responsible for onboarding new personnel, defining roles and positions of new hires, performing background checks, and facilitating the employee termination process.
Customer Success Department	• Responsible for the support of the Company's customers in their use of the service, including both managing customer programs and triaging incoming security vulnerabilities.
Product Department	• Responsible for the product lifecycle, including project management for development, design of user interfaces and experiences, and external documentation.

People	
Engineering Department	• Responsible for the development, testing, deployment, and maintenance of new code for the HackerOne Platform. • Responsible for access controls and security of the production environment. • Responsible for providing management of technical resource activities. • Responsible for providing technical resources to the Customer Success Department.
Finance Department	• Responsible for corporate IT.
Compliance Department	• Responsible for security and privacy compliance activities.

The following organization chart reflects the Company's internal structure related to the groups discussed above:

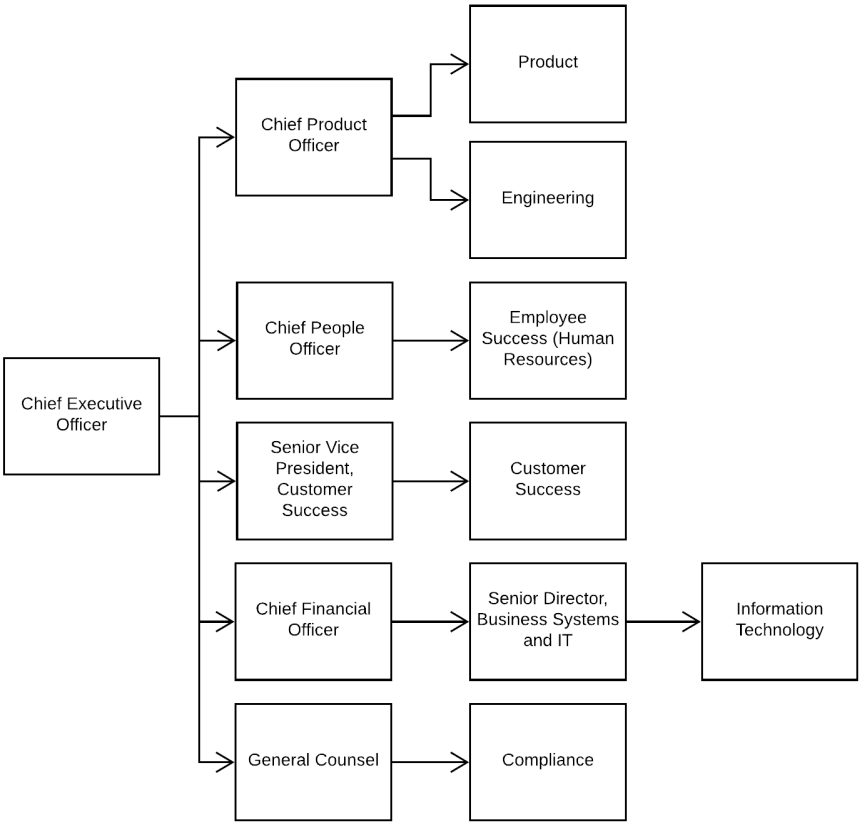

Figure 1: The Company's Organization Chart

PROCEDURES

Procedures include the automated and manual procedures involved in the operation of the HackerOne Platform. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), HR, etc. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

Procedures	
Procedure	**Description**
Logical and Physical Access	How the Company restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

DATA

Data is defined by the Company as:

- Vulnerability reports submitted by security researchers, including any associated metadata, attachments, and follow-up comments by any party.
- Personal information submitted by security researchers, including names, current and previous address details, online identifiers, tax identification number, nationality, date of birth, telephone number, financial information, payment information, etc.
- Personal information submitted by customers, including basic contact information, financial information, and banking information.
- Customer reports generated concerning activity on the HackerOne Platform, including penetration test reports.
- Credentials required for third party service integrations.
- User or organizational identifiable information, including email addresses and passwords, required for authentication and authorization decisions.
- Business information needed to support commercial relationships and transactions.
- Logs and metrics of activities and actions occurring, including Internet Protocol (IP) addresses.
- Analytics information, including user activity, browser information, and performance metrics related to use of the HackerOne Platform.

This data is loaded into the environment and accessed remotely from customer systems via the Internet. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential and/or sensitive information over public and private networks. Data stores housing customer data are encrypted at rest. Additionally, log files are retained to provide immutable records of computer events about an operating system, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by management to customers regarding the performance of the HackerOne Platform. Commitments are communicated via online Terms & Conditions (T&Cs) and in written Master Service Agreements (MSAs) and Service Level Agreements (SLAs), as well as the data and information security policy posted on the Company website.

System requirements are specifications regarding how the HackerOne Platform should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures, which are available to all employees.

The Company's principal service commitments and system requirements include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Maintain written security management policies and procedures to prevent, detect, contain, and correct violations of measures taken to protect the confidentiality, integrity, and availability of Company information systems and/or customer's confidential information. • Perform risk assessments for both internal and external threats to the HackerOne Platform and its information.	• Logical access standards • Physical access standards • Employee provisioning and deprovisioning standards • Access reviews • Encryption standards • Security training • Risk and vulnerability management standards • Configuration management • Incident handling standards • Change management standards • Vendor management • Systems development life cycle (SDLC)
Availability	• Be operational and available 24 hours per day, 7 days per week. • Maintain an uptime of 99.5% per calendar month except for scheduled maintenance and upgrades and excluding application program interface (API) interruptions or third-party system interruptions.	• System monitoring • Backup and recovery standards • Physical and environmental protections

Trust Services Category	Service Commitments	System Requirements
Confidentiality	• Maintain all customer data as confidential, not disclose confidential information to any unauthorized parties, and not use any confidential information for any purpose other than agreed-upon.	• Data classification • Retention and destruction standards • Data handling standards • Internal confidentiality standards • Information sharing standards