GreatHorn, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, and Confidentiality categories for the period of August 1, 2018 through October 31, 2018.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF GREATHORN, INC. MANAGEMENT

ASSERTION OF GREATHORN, INC. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within GreatHorn, Inc.'s Cloud-Based Email Security Solution System (system) throughout the period August 1, 2018, to October 31, 2018, to provide reasonable assurance that GreatHorn, Inc.'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 section 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 August 1, 2018, to October 31, 2018, to provide reasonable assurance that GreatHorn, Inc.'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*). GreatHorn, Inc.'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 section 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 August 1, 2018, to October 31, 2018, to provide reasonable assurance that GreatHorn, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Kevin O'Brien
Chief Executive Officer
GreatHorn, Inc.
260 Charles St, Ste. 300
Waltham, MA 02453

Scope

We have examined GreatHorn, Inc.'s accompanying assertion titled "Assertion of GreatHorn, Inc. Management" (assertion) that the controls within GreatHorn, Inc.'s Cloud-Based Email Security Solution System (system) were effective throughout the period August 1, 2018, to October 31, 2018, to provide reasonable assurance that GreatHorn, Inc.'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

GreatHorn, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that GreatHorn, Inc.'s service commitments and system requirements were achieved. GreatHorn, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, GreatHorn, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services 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 GreatHorn, Inc.'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 GreatHorn, Inc.'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 GreatHorn, Inc.'s Cloud-Based Email Security Solution system were effective throughout the period August 1, 2018, to October 31, 2018, to provide reasonable assurance that GreatHorn, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

November 26, 2018

GREATHORN, INC.’S DESCRIPTION OF ITS CLOUD-BASED EMAIL SECURITY SOLUTIONS SYSTEM

SECTION A:
GREATHORN, INC. 'S DESCRIPTION OF THE BOUNDARIES OF ITS CLOUD-BASED EMAIL SECURITY SOLUTION SYSTEM

Services Provided

GreatHorn has created a SaaS solution for cloud-native email security for Office365 and G Suite. The GreatHorn Threat Intelligence Platform offers advanced threat protection, cloud-native design, and continuous protection. The solution protects from advanced threats to its clients' network infrastructure, including phishing attacks leveraging social engineering. The GreatHorn Threat Intelligence Platform is cloud-based and can de deployed very quickly in client environments.

Infrastructure

The network diagram is created by the CTO and Infrastructure Engineer. It is also reviewed by the Vice President of Engineering. The diagram is reviewed and updated annually and with any major changes. Once the diagram is approved, it is reviewed with all other engineering and quality assurance team members. The network diagram captures the segregation of environments and the logical location of firewalls.

The organization maintains an inventory of all systems that make up the company's network. The inventory is updated by the CTO and Infrastructure Engineer when there are major changes in infrastructure or personnel.

Software

The organization maintains an inventory of critical software and licensing. The inventory is updated when there are changes in infrastructure and/or personnel.

The organization contracts with Stripe, a third-party payment application provider, to help with payments for a small number of customers. Stripe is in the VISA Global Registry of Service Providers with PCI DSS, Visa TPA program (HR ISO), and Visa TPA Program (ISO-M) validations types.

The organization uses formal application development processes for its solution. A code repository is utilized for version control of custom software. Jira is used to track individual tickets which are tied to a release. The development team is assigned, and the review and release assignment is made by the VP of Engineering, Development, QA, and Cloud Operations. Developers utilize local machines for development, utilizing Gitlab as a code repository with access limited to appropriate team members. The QA team pushes code to the Staging environment for quality assurance. Management must grant approval before code is moved to production by Infrastructure personnel.

The organization maintains separate development, staging, and production environments. Developers do their development locally, downloading a branch of staging to their laptops associated with a Jira ticket number as part of the naming convention standard. Code is pushed by

QA to staging for testing, approval, and tagging for production releases, which are pulled once approved by QA and Senior Management.

The organization utilizes secure application development procedures to ensure that applications are not vulnerable to external threats. These system development procedures include but are not limited to development, peer code review, CTO code review to catch security flaws, and approval. Once the CTO approves of code, quality assurance procedures are implemented. Code is automatically tested for functionality. Management approves the code, and it is moved to production. For major releases and new features, the review is done to identify security implications.

People

Management oversees the duties of all employees through a definite organizational structure. The company utilizes a flat structure due to the size of the company. Senior management report to the Chief Executive Officer and Cofounder. The Chief Technology Officer and Cofounder is involved in daily operations and also fills the role of the Chief Information Security Officer. The leadership team also incorporates Engineering, Controller/Finance, Operations, Marketing, Sales, and Business Development personnel.

The Board of Directors oversees strategy and governance. The Board consists of venture partners and the organization's cofounders. Meetings are held every six weeks.

Data

The organization documents the flow of data through the organization’s network. The dataflow diagram is updated annually and after any major changes. The Chief Technology Officer and the Infrastructure Engineer maintain the diagram.

The organization has a data classification system that ensures the secure handling of sensitive data. Data classification contains the requirements related to confidentiality, retention controls defining data elements, retention policy and additional information related to each element, and data disposal requirements and procedures. Data retention requirements meet the legal, regulatory, and business needs of the company, including those related to GDPR and HIPAA.

Sensitive data is encrypted during transit and at rest on the network. Data at rest is encrypted on the disk using AES 256. Databases at rest are using Amazon Web Services’ keys generated to their requirements. Data communication uses TLS/ECDHE key exchange with AES 256 and SHA-386. The communication between the organization's site and customer site is protected by an IPSec ESP tunnel using 168-bit TripleDES encryption with SHA-1 authentication. It utilizes either an out-of-band shared secret or PKI certificates. Data in transit to customer Office and G-Suite environments is protected by TLS 1.2 with redirection of HTTP to HTTPS.

Application service transactions are appropriately protected. procedure Application transactions are protected through the use of a unique event hash which prevents duplication of records on ingestion/update.

Processes and Procedures

Automated alerts and other network settings are evaluated in order to determine proper action and remediation. A daily stand-up meeting is used to provide a forum for the review of Threat Stack alerts and CVEs. The meeting has a goal of ticketing and remediation of at least two CVEs.

Every Friday personnel review the local network settings. Management reviews the settings for network and users. Tickets are logged for remediation activities. A daily review of dashboards and Azure and AWS environments is completed.

SECTION B:
PRINCIPLE SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Regulatory Commitments

The organization complies with all applicable regulatory measures. The organization is subject to GDPR as a Data Processor. If customers have HIPAA requirements, the organization will sign a Business Associates Agreement. Privacy principles are covered in Security Awareness Training. The organization's environment architecture supports compliance with GDPR. The privacy policy is updated to reflect compliance with guidelines.

Contractual Commitments

The organization commits to utilizing industry-standard security processes and procedures. Contractual material sets forth terms and conditions related to subscription, support, terms, renewals, and termination. The customer retains the rights, title, and interest in their own information and data. The organization has committed to confidentiality and compliance with applicable laws and regulations.

System Design

GreatHorn has designed their systems and environments utilizing highly secure and infrastructure-redundant cloud-based services. The organization has implemented industry-accepted hardening and encryption standards, segregation, monitoring, intrusion detection, and intrusion prevention.