# Final Report – Cymbal Bank Data Breach

This report presents the results of the investigation, containment, and recovery actions taken following the recent data breach at Cymbal Bank. The incident involved unauthorized access to cloud resources hosted on Google Cloud. The findings, responses, and lessons learned are outlined below.

## Executive Summary

Cymbal Bank faced a data breach that exposed sensitive customer and payment information. The breach occurred due to a combination of cloud misconfigurations — including a publicly accessible storage bucket, open firewall ports, and a Compute Engine instance with a public IP and disabled Secure Boot.  
  
The Security Command Center (SCC) detected the anomaly through compliance alerts and findings analysis. The Security Operations Team (SOC) acted immediately to isolate affected assets, eliminate risks, and restore secure operations. No persistent malware was found, and all systems were verified clean within 24 hours. This incident reinforced the importance of proactive monitoring, least-privilege access, and network segmentation.

## Investigation Summary

The investigation revealed that the attacker exploited multiple misconfigurations to gain access to Cymbal Bank’s Google Cloud environment. The following factors contributed to the breach:

* A compromised virtual machine (cc-app-01) with open SSH (22) and RDP (3389) ports allowed unauthorized access from the internet.
* A publicly accessible Cloud Storage bucket permitted unauthenticated global reads.
* The compromised VM used a default service account with excessive API access rights.
* Firewall rules (default-allow-icmp, default-allow-ssh, default-allow-rdp) were overly permissive, allowing inbound traffic from all IP addresses.
* The attacker briefly exfiltrated limited customer data before the SOC intervened.

## Containment and Eradication

* Immediately stopped the compromised VM (cc-app-01) and created a forensic snapshot for evidence preservation.
* Isolated the affected network to prevent lateral movement across environments.
* Deleted all broad firewall rules allowing 0.0.0.0/0 access to SSH, RDP, and ICMP.
* Revoked public access for all Cloud Storage buckets and removed the 'allUsers' and 'allAuthenticatedUsers' principals.
* Verified IAM roles, reducing privileges and removing unused service accounts.
* Updated SCC configurations to trigger alerts faster for public or high-risk resources.

## Recovery and Hardening

* Created a new hardened VM (cc-app-02) from a clean snapshot with Secure Boot and no public IP address.
* Deleted the compromised VM after evidence collection was complete.
* Enabled Uniform Bucket-Level Access (UBLA) on all Cloud Storage buckets for centralized access control.
* Implemented a new firewall rule 'limit-ports' restricting SSH to the Google IAP IP range (35.235.240.0/20).
* Enabled firewall logging for both 'limit-ports' and 'default-allow-internal' rules for full visibility.
* Executed a PCI DSS 3.2.1 compliance report to validate all remediations.
* Confirmed no additional threats or unauthorized connections were present after remediation.

## Recommendations and Lessons Learned

* Enable continuous monitoring in SCC to detect and alert on public exposures and IAM misconfigurations.
* Mandate multi-factor authentication (MFA) and enforce least-privilege IAM policies for all cloud users.
* Expand network observability with VPC Flow Logs and Chronicle SIEM integration for real-time threat correlation.
* Implement recurring incident response tabletop exercises to validate readiness and coordination among security teams.
* Regularly review firewall rules, IAM permissions, and Cloud Storage access lists to maintain compliance and security posture.

## Conclusion

Through rapid containment, methodical remediation, and continuous monitoring, Cymbal Bank successfully mitigated the data breach and restored secure operations. The security team demonstrated strong collaboration and effective use of Google Cloud tools such as SCC, Compute Engine, and IAM. The post-incident review confirmed that the implemented controls now meet PCI DSS and NIST CSF standards. Ongoing improvements in automation and logging will ensure future incidents are detected and resolved even faster.

Prepared by: Jeferson Domingues Madureira – Junior Cloud Security Analyst

Date: 28/10/2025