Issues for ID: IS-002722

Folder Path:
/Abc/US Businesses/Marketing/CMO-Chief Brand Office

ID:
IS-002722

Issue Rating:
High

Repeat Issue:
No

Root Cause Description:
The root cause can be attributed to both various VEM and organizational changes occurring over the past few years, which over time has impacted clarity regarding the applicable ongoing monitoring standards. Also, during the vendor onboarding process (2018) appropriate SaaS configuration was not performed.

Name:
Minimum third-party and privacy standards were not executed resulting in inadequate information security controls to prevent inappropriate access to customer information by internal or external parties.

Issue Owner.Display Name:
David Hamlett - david.hamlett@abc.com

Due Date:
2024-10-31 00:00:00

Description:
Sprinklr is a Software as a Service (SaaS) social media management platform used to implement social media strategy and support the tracking and triage of comments received from consumers (e.g., service requests, customer complaints). The Abc Social Media Listening Program uses Sprinklr to monitor social media content involving Abc across various public platforms (e.g., Facebook, LinkedIn). The Social Media team began collecting Personal Information (PI) to provide further customer assistance since 2018.

Based on testing performed, Internal Audit noted the following:
• Vendor Engagement Manager (VEM) didn't update the Inherent Risk Rating (IRR) for Sprinklr to reflect the collection of PI, therefore the required enhanced monitoring and due

diligence per Third-Party Risk Management Program and Standards wasn't performed. Similarly, a Privacy Impact Assessment (PIA) was not completed for Sprinklr. There were 173 (out of 11,160) cases during the scope period where PI was requested from the customer. Management has since completed the PIA as of February 2024.
• Sprinklr can be accessed from outside of the Abc network using personal devices through established credentials (username and password), therefore bypassing Enterprise authentication and information security controls, including data loss prevention. Additionally, multifactor authentication (MFA) as required by Enterprise standards was not in place at the time of the audit.
• While access to Sprinklr can be provisioned directly by certain users within the Social Media Operations team, a recertification has not been implemented; however, access at the application level was deemed appropriate.
• Access to Abc's specific social media account handles (public usernames) managed within the platform is not reviewed periodically to ensure appropriateness of user access and permissions. IA and management were unable to confirm the appropriateness of access at the time of the audit.

Issue Rating Rationale:

Without the appropriate vendor onboarding and oversight controls to ensure compliance with Company standards, key vendor, privacy, and information security risks may not be assessed and appropriately addressed which can result in privacy breaches or complaints. The misclassification of a vendor application and the resulting absence of information security controls increases the likelihood of unauthorized access and data breaches. Abc manages 59 social media accounts with combined followers totaling over 1.4 million, which increases the potential of significant reputational impact if an unauthorized user gains access to the application through either incorrect access provisioning or inadvertent exposure from access to the Abc network. Additionally, the collection and sharing of PI without adequate protection increases the risk of regulatory fines and litigation. These risks are partially reduced as there is a limited number of user licenses (24) available to provision access for the Sprinklr application. Further, based on management's re-assessment of the vendor IRR, it was estimated that the potential number of records containing PI within the engagement is currently limited to between 500 and 10k records, within a moderate risk range based on threshold established by the Privacy standards. As a result, the issue is rated "High" risk.

Risk Category:

8. Information Security

Issue Status:

Open

Additional Description:

nan

Operating Division:

US Businesses

Business Group:

Marketing

Reportable Segment:

CMO-Chief Brand Office

Action Plans ID:

['AC-003533', 'AC-003534', 'AC-003535', 'AC-003536', 'AC-003537', 'AC-003538', 'AC-003539', 'AC-003610']