Humberto Gonzalez

December 15, 2024

1. What PCI merchant level applies to SnowBe Online? Why? Be thorough in your explanation.

SnowBe Online is a PCI DSS Merchant Level 2 because it processes 1,200,000 credit or debit card transactions per year, which exceeds the Level 3 threshold (20,000 to 1,000,000 e-commerce transactions) but does not meet the Level 1 criteria (more than 6 million transactions or a significant breach history). The Level 2 designation is based on annual transaction volume and applies only to retailers who process between 1,000,000 and 6,000,000 card transactions per year across all channels.

2. What must SnowBe do under this level? Be thorough in your response.

- Complete an Annual Self-Assessment Questionnaire (SAQ): This questionnaire provides a complete assessment of their compliance with PCI DSS requirements. This applies to the storage, processing, and transmission of cardholder data on its AWS-hosted website, as well as physical shops that use PCI DSS-compliant terminals provided by their bank.
- Perform Quarterly Network Scans: Scans must be performed by an Approved Scanning Vendor (ASV) to identify vulnerabilities in external-facing systems. These scans attempt to identify vulnerabilities in the AWS-hosted website, as well as any systems or infrastructure that transmits cardholder data.

- Annually submit an Attestation of Compliance (AOC): The AOC must attest that SnowBe complies with all applicable PCI DSS requirements.
- * However, the level 2 merchant may seek an on-site PCI DSS audit and Report on Compliance (ROC) if the acquiring bank thinks it necessary.

3. Which SAQ(s) applies to SnowBe Online? Why? Be thorough in your explanation. If SnowBe Online is required to complete more than one SAQ, be sure to list and explain why for each. Be thorough in your explanation.

- SAQ D-Merchant- SnowBe retains credit card information on its AWS-hosted website and accepts payments online. This SAQ applies to retailers who store, process, or transmit cardholder data within their environment. SnowBe's use of AWS and the WordPress shopping cart for transaction processing makes them eligible for SAQ D. While the brick-and-mortar stores utilize bank-provided PCI DSS Level 1-certified terminals, SAQ D is applicable because it covers all parts of the company's activities that contain cardholder data. SnowBe maintains direct control over the e-commerce environment, therefore SAQ D addresses all requirements for both environments.

4. What else, if anything, is required based on the SAQ requirement? IF nothing, be sure to state that. Be thorough in your explanation.

Under SAQ D, SnowBe must ensure full compliance with all 12 PCI DSS requirements. According to the case. SnowBe has already established several controls, such as firmware updates, anti-virus software, and password changes, but additional measures may still be

necessary, these are some general PCI DSS requirements of the 12 requirements that are suited to SnowBe case study.

1. Encryption of stored cardholder data- Ensure that all cardholder data contained in the WP shopping cart is secured with strong encryption techniques.
2. Vulnerability Scan & Pen Test- Schedule quarterly vulnerability scans by an ASV (Approved Scanning Vendor) and annual penetration tests to identify and fix problems.
3. Incident Response Plan- Create and test an incident response plan to address breaches or potential breaches.
4. Access Controls- Implementing MFA for critical systems/all systems that need it. Ensuring that the right personal have the right privilege access level to systems that process cardholder data.
5. Loggin and Monitoring- Regularly review logs to detect unauthorized activity, and enable logging of all access to cardholder data and the critical systems.
6. Compliance Documentation- Document all needed documents for compliance and for auditing.
7. Security Awareness Training- Is critical for SnowBe since employees handle sensitive cardholder data.

In conclusion, SAQ D covers all components of SnowBe Online's cardholder data environment, so no additional SAQ is required. SnowBe must achieve full compliance with all 12 PCI DSS criteria outlined in SAQ D for its ecommerce platform and in-store payment processing. These measures ensure that sensitive data is protected and that the merchant is in compliance with PCI DSS standards at level 2.

5. Statement of agreement for the SAQ group portion. "I (Humberto Gonzalez) agree with the information that is in our group SAQ and agree to accept the grade that our group receives."