Humberto Gonzalez

November 24, 2024

Case Study Company: SnowBe Online

SnowBe Online is a lifestyle brand for those who love the beach and snow. The owners started the company with a laid-back culture. Their customers instantly connected with their brand taking them to $100 million in sales in three years. After being so successful, the management team decided to take the company public.

Technical Information:

1. The majority of their sales are processed online through their website, housed on the AWS platform.

a. All credit cards are accepted and stored on the company's website database.

b. All customer information and purchase history are stored on the website indefinitely.

2. They have multiple storefronts in the U.S. and Europe, which accept checks, cash, or credit cards. The credit card transactions are processed using bank-provided credit card terminals in each store.

3. There are twenty desktops and thirty laptops in the main office in Los Angeles.

a. The desktops are used to run the business and customer support.

b. The thirty laptops are used for sales (retail and wholesale). The laptops use a VPN to log into the office to access company applications.

4. There are six servers (on-premise and AWS) for access management, storage, customer relations management, order management, accounting, and vendor applications.

5. As a result of SnowBe's laid-back culture, they neglected to implement technical controls and processes. As a result, they recently hired a technical consultant to control their neglected system and processes. The consultant started with implementing controls using the NIST 800-53 r5 framework.

Additional Information:

The technical consultant was impressed to find a well-run company with no reported technical issues or breaches despite SnowBe's laid-back culture. Although, there had been a few attempts that did not cause any harm or alerts to worry anyone. The technical consultant analyzed the risk of the company using the NIST Risk Management Framework. Here are some initial steps he suggested:

- The need to update the firmware of all network devices.
- The need to update the patches for all PCs and Windows servers to ensure they use the latest Windows version.
- The need to update their Anti-Virus and backup software.
- The need to implement more processes into the access management system since most employees had access to almost all of the data on each server.
- The need to lock the servers in a secured area of the office.

- The need to update the company's WordPress shopping cart.

- The need to implement the required PCI compliance items.

- Login audit records need to be saved, and records older than 3 months should be archived to a cloud storage facility.

- Mobile devices need to be reviewed and approved to have access to the company data.