Humberto Gonzalez

December 15, 2024

Company Case Study: 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, which is housed on the AWS platform.

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

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

2. They have multiple storefronts in the U.S. and Europe, all of 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 on 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. They recently hired a technical consultant to assist with getting their neglected system and processes under control. The consultant started with implementing controls using the NIST 800-53 framework.

6. Due to SnowBe's laid-back culture, the technical consultant was impressed to find a well-run company with no reported technical issues or breaches. 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:

a. update the firmware of all network devices.

b. update the patches for all PCs and Windows servers so they are on the latest Windows version.

c. update their Anti-Virus and backup software.

d. implement more processes into the access management system since most employees had access to almost all data on each server.

e. lock the servers in a secured area of the office.

f. update the companies WordPress shopping cart.

Information added for week 2:

- The average size of sales is $75.
- Credit or debit purchases account for ninety percent of the sales, which equates to 1,200,000 transactions a year.

Information added for week 3:

- All the passwords have been changed, no default settings exist.
- All the desktop computers and laptop computers in each location have the same sign on information; however, each location is different from the others.
- The following recommendations from the technical consultant have been implemented.
    - The firmware of all network devices has been updated and properly configured.
    - The patches for all PCs and Windows server have been updated to ensure that they are on the latest Windows version.
    - The Anti-Virus software has been updated. No change to the backup software though.

Assumptions:

- Any items that have been corrected are no longer accessible without specific permission.
- Any payment that is not processed through their website is either cash or check.

- All sales are via the website or in person at a brick and mortar store; there are no MOTO transactions.
- The brick and mortar storefronts do not store any customer data.
- The bank-provided credit card terminals are PCI DSS Level 1 certified.
- AWS is certified as a PCI DSS Level 1 Service Provider, the highest level of assessment available.
- The Word Press shopping cart resides on SnowBe's web server.