CSO Scenario

Albertsons Companies

Jake O’Connor

UAT MS507

Assignment 4

Organization Definition

Albertsons Companies operates multiple chains of grocery stores, pharmacies, and fuel stations across most of the United States, most notably through brands Albertsons and Safeway. With over 2,200 stores across 34 states and a majority market share in most states served (*Corporate Profile*), Albertsons has the responsibility to guarantee a significant amount of private user data is protected from unauthorized use and to prevent major outages of service that would prevent customers from securing food, fuel, or medicine in a timely manner.

Network and Application Security

The large number of physical locations within the Albertsons Companies brand leads to a complex security strategy. With warehouses, retail locations, corporate offices, and data centers across the country at play there are a wide range of potential security threats to the organization. These basic security considerations can help keep the organization and its data secure from actors both internal and external, and help prevent data breaches that would result in violations and fines.

Device Access Control

Firewalls should be used to block incoming connections between buildings, servers, and locations. Devices should be allow-listed based on their need within the organization and who they are assigned to. As the company doesn't do business overseas, foreign IP addresses can be entirely blocked from accessing all but the most surface elements of the network.

User Access Control

Users should be required to maintain strong passwords and multi-factor authentication in order to access the company network. Access to data should be restricted to those who need access using

protocols assigned to each user based on their need. Access to facilities should be secured physically to prevent intrusion into devices that could lead to a bigger breach.

Email Security

Emails are a major vector of cyberattack, virus, and malware introduction. Company email accounts should be heavily secured, and personal email should not be allowed on secure company devices to prevent access to less secure external email accounts. Staff should undergo regular training on the identification of phishing and scam emails.

Antivirus/Antimalware

At the end of the day, something is going to slip through the cracks. To this end, all company devices should be outfitted with modern antivirus and antimalware software which is kept up to date with all new patches and upgrades. Security software should run silently on all user machines and expose no controls for employees to disable or otherwise pause protection.

Defense-in-Depth Structure

Since Albertsons Companies has such a large number of locations each serving different purposes, each should have their own specific security structure. For the sake of simplicity, the following will apply to all physical Albertsons Companies locations including warehouses, retail locations, and office buildings that host any kind of data.

Storage

Starting at the root of the structure, the storage of data is key. Only the minimum necessary data should be stored in the first place, limiting the worst-case scenario of a data breach. All databases should be highly encrypted and regularly backed up, further limiting the fallout from a cyberattack

which copies or destroys data. Where possible, data should be hosted at more secure facilities and only accessed via terminals in less secure locations.

Access

Data should only be accessible by users with valid credentials and a need to access such data. User account authentication should require a minimum complexity of password that suites the organization, and users should be required to make use of multi-factor authentication wherever possible. Once authenticated, only users authorized to access data should be allowed to access data. For example, users not part of the pharmacy organization should never be authorized to access customer healthcare data even if they are allowed to access the customer's other personal information.

Device

At the device level, there are multiple layers of security that should be applied. Only company devices should be allowed to access any secure data. Company devices should all be installed with security software that finds viruses, malware, and other malignant installs. Company devices should also be kept up to date with all security and stability patches for their respective operating systems. The installation of unknown software on company devices should be limited, and any authorized software that is installed should be kept up to date.

Network

The network level has one of the largest surfaces for vulnerability within the organization. Firewalls around each database and each location should exclude all unexpected communication from devices both internal and external. Communication between networks at different locations should be encrypted end-to-end.

Physical

Each different Albertsons Companies location has different physical security needs, but in each location the protocol should boil down to: no unauthorized users in secure areas. At warehouses and corporate offices any access to the facility should require a key or badge, and guests should be limited and tracked. Locations with databases and servers should have further security in and around those devices, such as added security doors. In locations with the expectation of customers and foot traffic, any access to employee-only sections of the business should be restricted with keys or badges. Retail locations with pharmacies should further restrict access to pharmacy areas to only those who work in the pharmacy.

Policy

At a policy level, Albertson's Companies employees need to be trained on security standards and held accountable to them. The user authentication password policy should require a strong, secure password and mandatory multi-factor authentication. Employees should be trained regularly on identifying phishing, scams, and suspicious emails and websites, and should know where and how to report such information. Clear usage policies should be put in places and adequately communicated, especially when it comes to customer data and health information.

References

Chaudhary, R. (2015, September 22). *The 5 Essential Elements of Cybersecurity*. Crowe LLP. https://www.crowe.com/cybersecurity-watch/5-essential-elements-cybersecurity.

Corporate Profile. Albertsons Companies: Corporate Profile. (n.d.). https://investor.albertsonscompanies.com/corporate-profile/default.aspx.

Five key elements of effective network security. Black Box. (n.d.). https://www.black-box.eu/en-int/page/23903/Resources/technical/Black-Box-Explains/security/five-key-elements-of-effective-network-security.

Smith, T. (2015, November 6). *The Most Important Elements of Application Security - DZone Security*. dzone.com. https://dzone.com/articles/the-most-important-elements-of-application-securit.

Wireman, M. (2013, May 16). *NIST and Web Application Security:Is Your Organization Really Considering All of the Risks in the Enterprise?* CISO Platform. https://www.cisoplatform.com/profiles/blogs/nist-and-application-security-is-your-organization-really.