CSO Scenario

Albertsons Companies

Jake O’Connor

UAT MS507

Assignment 2

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 (*Albertsons Companies Company Fact Sheet* 2020), 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.

Laws and Regulations

With over thirty million weekly customers across the United States, thousands of pharmacies dealing with patient healthcare information, options for home delivery and curbside-pickup in most services areas, and a customer loyalty program, Albertsons Companies is responsible for the security of a staggering amount of user data that needs to be secured properly in order to adhere to the various laws and regulations throughout the different jurisdictions within the United States. The following four laws, regulations, and standards are just a few of those which may need to be followed by Albertsons Companies in order to ensure that customer data is properly secured and to avoid harsh penalties.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA), established in 1996, outlines a large set of requirements for organizations and individuals dealing with patient medical records, ranging from how records are stored to when and how records can be disclosed between organizations and individuals (*Health Insurance Portability and Accountability Act of 1996 (HIPAA)* 2018). Albertsons Companies stores serve millions of pharmacy customers per year, most in filling prescriptions and providing over-the-counter medications, and as such has access to and responsibility for a large amount

of HIPAA-protected customer healthcare data. On the cybersecurity front, ensuring that patient healthcare records are stored securely, and that the transmission of those records between different stores both inside and outside of the Albertsons Companies network and to and from healthcare providers, is paramount in ensuring that HIPPA regulations are adhered to.

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA), established in 2018, outlines four primary privacy regulations for businesses which serve residents of California: the right to know, right to delete, right to opt-out, and right to non-discrimination (California Consumer Privacy Act (CCPA) 2021). Albertsons Companies operates five separate chains of grocery store and pharmacy in the state of California, and as such is obligated to follow the regulations set out in the CCPA. The CCPA generally aims to protect consumers from having their private data, such as social security numbers, bank details, and medical records, collected and transferred without their consent. While the CCPA does not explicitly limit the types or amount of personal data that can be collected, it does put the onus on the company to securely store collected data, clearly notify consumers of what data is collected and why, clearly notify consumers of what data is sold or transferred to business partners and provide consumers a way to opt-out of data collection and have their collected data deleted.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS), established in 2006, is a set of standards for companies of any size that accept credit, debit, or prepaid cards that outlines rules and regulations for the secure storage and use of payment cards (PCI Compliance Guide Frequently Asked Questions: PCI DSS FAQs 2017). With over thirty million monthly customers across the United States, and payment cards being the preferred mode of payment by most consumers, Albertsons Companies has a large responsibility to ensure that all their stores are compliant with the PCI DSS in order to secure

their customers' data and avoid the fines and loss of public opinion associated with a breach of compliance. The PCI DSS compliance standards offer a large number of best practices for securing customer card data regardless of how that data is used, such as the use of third-party credit card vault providers or storing the bare minimum of user financial data and highly encrypting it.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), established in 2018, is a set of consumer protection regulations created by the European Union in order to protect the personally identifiable data of EU citizens both in Europe and across the globe (GDPR - User-Friendly Guide to General Data Protection Regulation 2020). Though Albertsons Companies does not operate any stores in continental Europe, the scope of the GDPR can and does extend to companies worldwide that do business with citizens of the EU. Albertsons Companies operates multiple globally accessible websites for their different chains of stores and operates hundreds of stores in areas trafficked by EU tourists, and as such could easily be considered to be marketing to or trading with citizens of the EU. Regardless of applicability of the GDPR to Albertsons Companies, operating as though the regulations apply and ensuring that the minimum viable amount of consumer data is collected, ensuring consumers are aware of that data collection, and ensuring that any collected data is secured against breaches will help to guarantee that Albertsons Companies avoids fines and loss of consumer trust.

NIST Publications

With retail stores, pharmacies, fuel stations, distribution centers, and manufacturing plants, Albertsons Companies has countless threat vectors for cyber-attacks and a large potential impact due to those threats. Almost any of the peer reviewed NIST publications could be used to inform the creation and maintenance of a secure network infrastructure for Albertsons Companies. The following three NIST

special publications are just a small subset which serve to provide a varied coverage for all the aspects of Albertsons Companies infrastructure.

Cyber Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161)

Special Publication 800-161, *Cyber Supply Chain Risk Management Practices for Systems and Organizations*, covers topics associated with the management of threat vectors created by the addition of third-party devices and software to a company's network (Boyens et al., 2021). With an increasing reliance on third-party tools to supplement the network infrastructure and operations of an ever-growing network of stores, warehouses, and manufacturing plants so increases the potential exposure to risk from third-party tools to the overall supply chain. This publication provides guidance on cyber supply chain risk management (C-SCRM) practices and policies for how to best manage a broad, multilayered network of technologies while assessing and mitigating potential risks to the overall supply chain.

Securing Web Transactions: TLS Server Certificate Management (SP 1800-16)

Special Publication 1800-16, *Securing Web Transactions: TLS Server Certificate Management*, covers topics associated with the management of the hundreds and thousands of TLS certificates that any medium or large enterprise ends up making use of to help secure their network transmissions both internally and externally (Akram et al., 2020). With thousands of stores and pharmacies across the country dealing with millions of customers' data on a daily basis, and the need for secure transmission of that data between any of thousands of different endpoints, Albertsons Companies must manage a vast number of TLS certificates to help ensure the security of data transfer. This publication provides guidance on best practices for establishing a structured certificate inventory, the application of

continuous monitoring of certificate status and security, and processes for the quick migration to new certificates when vulnerabilities or breaches are found within the network of TLS certificates.

Securing Electronic Health Records on Mobile Devices (SP 1800-1)

Special Publication 1800-1, *Securing Electronic Health Records on Mobile Devices*, covers topics associated with ensuring the sanctity and security of patient health records while making use of the conveniences of mobile devices (O'Brien et al., 2018). Albertsons Companies has more than seventeen hundred pharmacies across the United States and employs thousands of pharmacists and pharmacy technicians to provide services ranging from prescription filling to consultations to vaccine administration. This large number of pharmacies, customers, and healthcare-adjacent employees, as well as the increased usage of mobile devices for storage, transmission, and storage of healthcare information, creates a large surface area for potential cybersecurity threats for Albertsons Companies. This publication provides a modular framework of best-practices for using open-source and commercially available technologies in order to best provide security to mobile devices handling patient healthcare information while minimizing impact to the efficacy of those mobile devices.

References

Akram, M., Barker, W., Clatterbuck, R., Dodson, D., Everhart, B., Gilbert, J., Haag, W., Johnson, B., Kapasouris, A., Lam, D., Pleasant, B., Raguso, M., Souppaya, M., Symington, S., Turner, P., & Wilson, C. (2020, June 16). *Securing Web Transactions: TLS Server Certificate Management*. CSRC. https://csrc.nist.gov/publications/detail/sp/1800-16/final.

Albertsons Companies. (2020). *Albertsons Companies Company Fact Sheet*. ABSCos_Company-Fact-Sheet_Q4-2020_042621.pdf.

https://s25.q4cdn.com/593003593/files/doc_downloads/2021/04/ABSCos_Company-Fact-Sheet_Q4-2020_042621.pdf.

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

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2021, April 29). *Cyber Supply Chain Risk Management Practices for Systems and Organizations*. CSRC. https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft.

California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General. (2021, March 3). https://www.oag.ca.gov/privacy/ccpa.

Centers for Disease Control and Prevention. (2018, September 14). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Centers for Disease Control and Prevention. https://www.cdc.gov/phlp/publications/topic/hipaa.html.

GDPR - User-Friendly Guide to General Data Protection Regulation. GDPR EU. (2020, December 21). https://www.gdpreu.org/.

Newhouse, W., Bartock, M., Cichonski, J., Ferraiolo, H., Souppaya, M., Brown, C., Dog, S., Prince, S., & Sexton, J. (2019, August 27). *Derived Personal Identity Verification (PIV) Credentials*. CSRC. https://csrc.nist.gov/publications/detail/sp/1800-12/final.

O'Brien, G., Lesser, N., Pleasant, B., Wang, S., Zheng, K., Bowers, C., Kamke, K., & Kauffman, L. (2018, July 27). *Securing Electronic Health Records on Mobile Devices*. CSRC. https://csrc.nist.gov/publications/detail/sp/1800-1/final.

PCI Compliance Guide Frequently Asked Questions: PCI DSS FAQs. PCI Compliance Guide. (2017, September 5). https://www.pcicomplianceguide.org/faq/.

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2021, January 28). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. CSRC. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.