CSO Scenario

Albertsons Companies

Jake O’Connor

UAT MS507

Assignment 1

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.

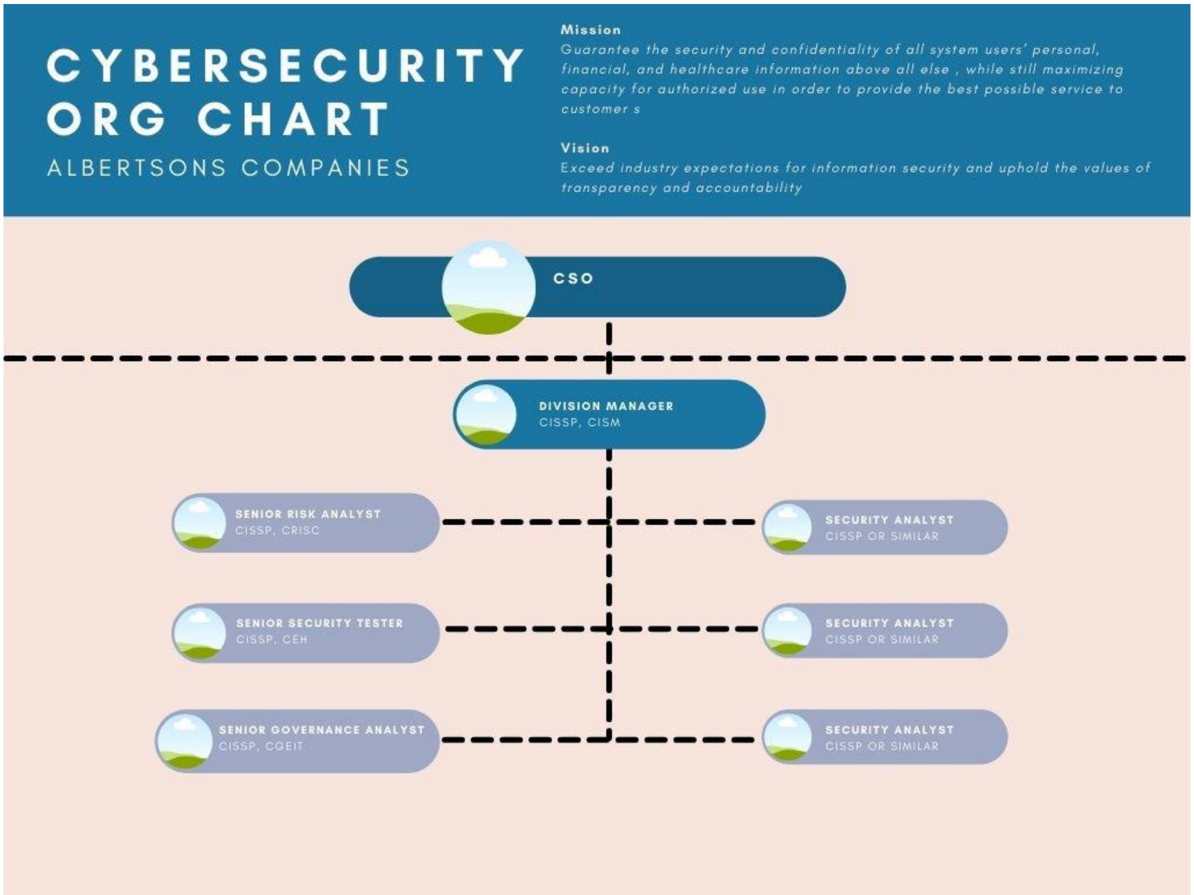
Cybersecurity Mission and Vision

The mission and vision statements of the Albertsons Companies brands are truly awful for how successful the companies are, but the driving values of the company as a whole can be used to build out adequate cybersecurity-focused mission and vision statements. Albertsons Companies aims to ensure that "customers, employees, and … business partners – are treated with Courtesy, Dignity, and Respect" (*Our Values*). These values can directly extend into the cybersecurity goals, as a breach of cybersecurity, especially one that exposes customer, employee, or business partner information, would be a devastating hit to their respect for the organization.

The first mission statement of the newly established cybersecurity department of Albertsons Companies would be *to guarantee the security and confidentiality of all system users' personal, financial, and healthcare information above all else, while still maximizing capacity for authorized use in order to provide the best possible service to customers*. This statement puts the Albertsons Companies primary values, compliance laws, and customer expectations at the forefront while keeping in mind the need to provide customers with the best possible service.

The vision statement for the newly established cybersecurity department of Albertsons Companies would be *to exceed industry expectations for information security and uphold the values of transparency and accountability.* This vision keeps with the expectation of the department's mission statement focusing on a high degree security for customer, employee, and business partner information while also focusing on raising the bar for the industry as a whole. The future goals for the cybersecurity department follow this vision statement. The first goal, physically separating user data into databases based on each of the thirteen geographic and brand divisions within the Albertsons Companies family, will help to mitigate the worst-possible effects of a cyber-attack, natural disaster, or outage by limiting the total effect to only a portion of users, as well as simplifies restricting authorized access to data based on division. The second goal, ensuring end-to-end encryption of all user data between the point-of-sale, database, and website, with additional layers of security for all financial and healthcare data, will help guarantee compliance with applicable laws and ensure protection of customer privacy.

Cybersecurity Organization Chart



CYBERSECURITY ORG CHART

ALBERTSONS COMPANIES

Mission

Guarantee the security and confidentiality of all system users' personal, financial, and healthcare information above all else , while still maximizing capacity for authorized use in order to provide the best possible service to customer s

Vision

Exceed industry expectations for information security and uphold the values of transparency and accountability

CSO

DIVISION MANAGER
CISSP, CISM

SENIOR RISK ANALYST
CISSP, CRISC

SENIOR SECURITY TESTER
CISSP, CEH

SENIOR GOVERNANCE ANALYST
CISSP, CGEIT

SECURITY ANALYST
CISSP OR SIMILAR

SECURITY ANALYST
CISSP OR SIMILAR

SECURITY ANALYST
CISSP OR SIMILAR

The proposed organizational chart for the new cybersecurity department of Albertsons Companies is divided into individual units per division, with the total size of the unit coming down to the overall security need of that division. Loosely, each division's cybersecurity team is helmed by a division manager who is an IT security professional specializing in management. Within each team are a series of specialists, one specializing in risk assessment and management, one in IT governance, and one in ethical hacking and security testing. Along with these specialists, each team will have a number of security generalists all holding a minimum set of certifications ranging from SSCP to CISSP.

Cybersecurity Team Certifications

CISSP – Certified Information Systems Security Professional

The CISSP is a general, process-oriented certification for IT security professionals with experience in the field. It certifies a nominal level of knowledge in each of eight different security domains and holders are expected to be capable of designing and creating effective security systems. (*CISSP - Certified Information Systems Security Professional*) Each senior-level position in the cybersecurity organization will be required to possess and maintain a CISSP (or equivalent alternative) in order to certify their continued knowledge of common security practices and processes.

CISM - Certified Information Security Manager

The CISM is a security certification focused primarily on the leadership and management of IT and cybersecurity professionals as well as guarantees a broad base of knowledge in the security field. It certifies a nominal level of knowledge across four different domains with a focus on management and leadership of a cybersecurity team based on industry best practices. (*CISM - Certified Information Security Manager*) Each team manager within the cybersecurity organization will be required to possess and maintain a CISM (or equivalent alternative) in order to certify their continued knowledge of best practices in the management of a team of cybersecurity professionals and secure IT network.

CEH - Certified Ethical Hacker

The CEH is a security certification focusing on ethical hacking methodologies and the lawful penetration testing of software and services. It certifies a nominal level of knowledge across a broad base of skills and tools required to test the security of software systems withing an organization. (*CEH - Certified Ethical Hacker v11*) Each team within the cybersecurity organization will have at least one senior analyst focusing on security testing, and that analyst will be expected to possess and maintain a

CEH (or equivalent alternative) in order to certify their continued knowledge of ethical hacking and penetration testing best practices.

CGEIT - Certified in the Governance of Enterprise IT

The CGEIT is a security certification focusing on the governance and management of enterprise IT and IT resources within an organization. It certifies a nominal level of knowledge across four distinct domains from IT resource management to risk optimization. (White, 2018) Each team within the cybersecurity organization will have at least one senior analyst focusing on IT governance for the division, and that analyst will be expected to possess and maintain a CGEIT (or equivalent alternative) in order to certify their continued knowledge of best practices in the governance of enterprise IT resources.

CRISC - Certified in Risk and Information Systems Control

The CRISC is a security certification focusing specifically on the identification and management of risks within the IT organization. It certifies a nominal level of knowledge across four domains from risk management to incident response. (*CRISC - Certified in Risk and Information Systems Control*) Each team within the cybersecurity organization will have at least one senior analyst focusing on the unique risk vectors of that division, and that analyst will be expected to possess and maintain a CRISC (or equivalent alternative) in order to certify their continued knowledge of common industry practices regarding risk management and security governance.

Cybersecurity Hiring Questions

Explain the differences between Authentication and Authorization and how they affect IT security.

Candidate's answer should cover at least the following concepts. Authentication is the verification of a valid user's identity. Authorization is the verification that a valid user should have access to a specific business asset or piece of data. Authentication and Authorization work together to ensure that only users that can be confirmed to exist within the system, possess valid access credentials, and are meant to be able to access the requested systems or data are allowed to.

Explain some common requirements for mobile devices that access secure IT systems.

Candidate's answer should include at least the following concepts. The use of an approved VPN in order to access any company resources from a mobile network. The ability to perform a remote lock-out and/or remotely wipe all relevant data from a device in the event of an active or likely security breach.

Explain social engineering and its role in cybersecurity best practices.

Candidate's answer should include at least the following concepts. Social engineering in this context is the process of bypassing security procedures through the manipulation of employees and users. Social engineering can take the form of cold calls, phishing emails, fake social media profiles, and many other things. Cybersecurity best practices regarding social engineering are focused on the training of employees to better recognize potential social engineering attacks and to defer to the cybersecurity or IT team if there are any concerns.

Explain the concept personally identifiable information (PII) and its role in cybersecurity.

Candidate's answer should include at least the following concepts. PII is information that alone or with other data can uniquely identify a single individual. Certain sensitive PII, such as Social Security Numbers and medical records, need to be closely guarded by organizations in order to both maintain public trust and to adhere to many different local and national laws and regulations. Bonus points if they mention the European Union's General Data Protection Regulation (GDPR) and how it might affect the company even though it is in a different country.

Explain who should have access to detailed user data within an IT system.

Candidate's answer should essentially boil down to "only those individuals whose roles within the company directly require access to that information." If their answer is as simple as anyone above a certain level, that's a red flag.

References

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.). Our Values. https://www.albertsonscompanies.com/our-values.html.

CEH - Certified Ethical Hacker v11. Certified Ethical Hacker Training | CEH Certification | Global Knowledge. (n.d.). https://www.globalknowledge.com/us-en/course/91508/ceh-certified-ethical-hacker-v11/.

CISM - Certified Information Security Manager. Certified Information Security Manager Training | CISM | Global Knowledge. (n.d.). https://www.globalknowledge.com/us-en/training/certification-prep/topics/cybersecurity/section/isaca/cism-certified-information-security-manager/.

CISSP - Certified Information Systems Security Professional. Certified Information Systems Security Professional | CISSP | ISC2 | Global Knowledge. (n.d.). https://www.globalknowledge.com/us-en/training/certification-prep/topics/cybersecurity/section/isc-2/cissp-certified-information-systems-security-professional/.

Columbus, L. (2019, August 28). *Top 10 Most Popular Cybersecurity Certifications In 2019*. Forbes. http://www.forbes.com/sites/louiscolumbus/2019/08/28/top-10-most-popular-cybersecurity-certifications-in-2019/.

CRISC - Certified in Risk and Information Systems Control. Certified in Risk & Information Systems Control Train Online | Global Knowledge. (n.d.). https://www.globalknowledge.com/us-en/training/certification-prep/topics/cybersecurity/section/isaca/crisc-certified-in-risk-and-information-systems-control/.

Kim, D., & Solomon, M. (2018). *Fundamentals of information systems security* (3rd Edition). Jones & Bartlett Learning.

The Top Cybersecurity Certifications in 2021. Security Boulevard. (2021, January 5). https://securityboulevard.com/2021/01/the-top-cybersecurity-certifications-in-2021/.

White, S. K. (2018, December 5). *What is CGEIT? A certification for seasoned IT governance professionals*. CIO. https://www.cio.com/article/3325203/what-is-cgeit-a-certification-for-seasoned-it-governance-professionals.html.