## Cigna’s Cyber Security

**Industry information**

The health insurance industry is a complex and rapidly changing sector of the economy.

Health insurance companies provide a vital service by helping to finance the cost of medical care for their policyholders [1]. In recent years, the industry has come under pressure from various forces, including rising health care costs, competition from other types of insurance companies, and changing government regulations.

Cigna is one of the largest health insurance companies in the United States [2]. The company offers a wide range of health insurance products and services for individuals, families, and businesses. Cigna has over 15 million customers and operates in more than 30 countries.

Cigna's products and services include medical, dental, vision, and life insurance; health care and wellness programs; and pharmacy benefits management. The company also offers a variety of other insurance products, such as property and casualty, workers' compensation, and disability insurance. There have been several major cyber breaches in the health insurance industry in recent years. In 2015, Anthem, Inc., one of Cigna's major competitors, suffered a data breach that affected over 80 million people. In 2016, another major health insurer, Premera Blue Cross, was breached, affecting over 11 million people. These breaches have led to increased scrutiny of the health insurance industry's cybersecurity practices.

**Cigna Breaches**

Cigna has not suffered a major data breach in recent years. However, the company has been the target of several cyber-attacks. In 2012, Cigna's website was hacked and personal information of some customers was exposed [3]. In 2015, Cigna was the target of a phishing attack that led to the exposure of customer data. And in 2016, Cigna's email system was breached, leading to the exposure of customer data.

These attacks have led to increased scrutiny of Cigna's cybersecurity practices. The company has been working to improve its security posture in recent years, and has implemented a number of new security measures.

**Number of Employees**

Cigna is a large, international health insurance company with over 50,000 employees. The company offers a wide range of health insurance products and services, and has over 15 million customers.

**Cigna’s Main Lines of Business**

Cigna's main lines of business are health insurance, dental insurance, vision insurance, and life insurance. The company also offers health care and wellness programs, pharmacy benefits management, and a variety of other insurance products.

**Significant Information Systems**

Cigna's significant information systems include its customer database, claims processing system, and website. The company also has a number of internal systems for employees, such as its email system and human resources system.

**Cigna's Headquarters Location**

Cigna's headquarters are located in Bloomfield, Connecticut, USA.

**Significant Information Regulatory Concerns**

The health insurance industry is subject to a number of regulatory concerns, including data security and privacy. In the wake of the Anthem and Premera data breaches, there has been increased scrutiny of the industry's cybersecurity practices [4]. Cigna has been working to improve its security posture in recent years, and has implemented a number of new security measures.

### References

1. H. W. L. Calvin J. Ali and K. Caals, "Ensuring trustworthy use of artificial intelligence and big data analytics in health insurance," Bulletin of the World Health Organization 98, no. 4 (2020): 263.
2. B. Denrick, K. Hatzitaskos B. T. Howells and A. Nevo, "The Aetna-Humana Proposed Mergers (2017)," JE Kwoka, Jr. and LJ White, The Antitrust Revolution: Economics, Competition, and Policy, (2019): 24-44.
3. S. Thomas A. F. Tadesse and N. E. Vincent, "The impact of CIO characteristics on data breaches," *International Journal of Accounting Information Systems* 43 (2021): 100532.
4. L. Zeyi, "“Success Is Invisible, But Failure Is Public”: Examining The US Office Of Personnel Management Data Records Breach," PhD diss., 2018.