Olivia Elder

Bryon Steinwand

Application Security

11/7/2024

Delta Dental

Data security is critical in industries like healthcare and insurance, where sensitive personal financial information is stored and processed. Healthcare care breaches are particularly alarming because they expose individuals to identify theft, financial fraud, and even medical identity theft. Cybercriminals are increasingly targeting these areas due to the high value of PHI, protected health information, on the black market. Data breaches can cause significant and long-lasting harm to both the customers and the company itself. Customers affected by the breaches may face identity theft, financial losses, and emotional distress. The organizations who are breached have their reputations damaged, face regulatory fines, and must deal with the costs of remediation. Furthermore, incidents like this prompt stricter enforcement of laws such as HIPAA, Health Insurance Portability and Accountability Act and PCI DSS, Payment Card Industry Data Security Standard. HIPAA was established to create federal standards protecting sensitive health information from disclosure without a patient’s consent while PCI DSS is a set of rules and guidelines that protects consumer’s credit cards.

A data breach occurs when unauthorized access to sensitive, confidential, or protected information is achieved. This could involve theft, exposure, or destruction of data without consent. Breaches within sectors like healthcare and insurance pose significant risks due to the fact data in these sectors often includes PII, personally identifiable information and PHI, protected health information. There are many categories of data that is exposed in a data breach. For example, personal identifiable information like names, social security numbers, addresses, and birthdate. Financial information is another category where credit card numbers, banking details, and insurance claims are also stolen. Healthcare data, which contains PHI, like medical records, treatment histories and diagnostic information is stolen. Credentials are another category containing usernames, passwords, and security questions which can lead to further attacks.

A major data breach in 2023 at Delta Dental raised concerns about the adequacy of the company’s cybersecurity measures. While exact details are still emerging, the breach underscores the vulnerabilities faced by the organizations that handle sensitive information. Delta Dental is one of the largest dental insurance providers in the United States, covering millions of people nationwide. Delta Dental operates 39 separate entities across all 50 states while holding approximately 25% of the dental insurance market. With its vast customer base, the company is responsible for safeguarding significant amounts of sensitive data, including names, addresses, social security numbers, and billing information. Their large customer base is what makes it an attractive target for cybercriminals.

Data breaches are very important because of the impact that they cause. There is the consumer impact where victims of data breaches often experience financial losses, emotional distress, and the consumer can face a long recovery process from the identity theft. It also has an impact on company that is breached, as they often face financial penalties, they can lose the trust of the consumer, and their reputation can be damaged. High profile breaches often prompt and increase scrutiny from regulators and a demand for stricter compliance requirements. This paper will analyze the Delta Dental data breach with an overview of what happened, identifying weaknesses in Delta Dental’s cybersecurity, and future recommendations. The Delta Dental breach reveals the need for comprehensive cybersecurity measures across industries.

Some common causes of data breaches are phishing attacks which are fraudulent emails that trick employees into revealing sensitive information or clicking malicious links. A more targeted phishing attack is called whaling, where the cybercriminals impersonate an executive to trick employees into revealing sensitive information. Ransomware attacks are when cybercriminals encrypt data and demand payment to restore access. Weak passwords are also a common cause, poor password practices allow hackers to gain unauthorized access to systems. An insider threat is when employees or third-party vendors intentionally or unintentionally expose sensitive data. Outdated systems with unpatched vulnerabilities create easy entry points for attackers. In the case of the Delta Dental breach, the attackers were able to use a SQL injection vulnerability with a software called MOVEit to access and download sensitive patient data.

The healthcare and insurance industries are particularly vulnerable because they manage large amounts of high value data making them desirable targets. There are also strict compliance requirements like HIPAA and PCI DSS add more responsibilities. Many organizations operate on outdated or fragmented IT infrastructures. However, outdated or fragmented IT infrastructures coupled with rapid technological advancements, often leave organizations unprepared for sophisticated cyberattacks. In Delta Dental case, they believed they were well prepared, but the file transfer software, MOVEit, was exploited by the hackers. This was known as a zero-day exploit because this vulnerability was previously unknown and so they were able to continue to exploit once found until a patch was available. Despite regulations data breaches continue to happen due to rapid technological advancements which often outpace an organization’s ability to adapt security measures. Human error, with poor passwords or falling to phishing attacks remains a significant vulnerability, which did not apply in Delta Dental’s case. Increasing sophistication of cyberattacks, including the use of AI and advanced malware challenges existing defenses. Delta Dental’s breach fits into these broader trends of cybersecurity challenges in the insurance industry.

Delta Dental is one of the largest dental insurance providers in the United States serving millions of individuals, families, and employer groups. The data responsibilities which Delta Dental handles consists of extensive sensitive information, including customer names, social security numbers, birthdates, addresses, dental and financial records, which is the type of material that was attained by the hackers. It also collaborates with healthcare providers, employers, and third-party vendors, expanding its data sharing network. The way that they do all these tasks like claims, billing, and customer service through digital platforms makes cybersecurity very important.

The discovery of this breach started when Delta Dental detected suspicious activity in its systems, triggering an internal investigation. The breach was determined to involve unauthorized access to customer and employee data. Although the mainly affected Delta Dental, the breach follows a broader wave of attacks by the Russian-linked C10p group, which also impacted other major organizations using the MOVEit software. The stolen data was made available on the dark web, increasing the potential risks for the affected individuals, including identify theft and fraud. In May 27-30, 2023, Hackers exploited a flaw in the MOVEit software to access sensitive data from Delta dental. On June 1st, 2023, Delta Dental became aware of the breach. On July 6th, 2023, an internal investigation confirmed the breach and identified the compromised data, which included names, social security numbers, addresses, financial information, and health related details. On November 27th, 2023, the investigation concluded, and Delta Dental completed its internal assessments. On December 14th, 2023, Delta Dental officially notified affected individuals and law enforcement about the breach. To address the incident, Delta Dental offered two years of free credit monitoring and identity theft protection for affected individuals.

The Delta Dental data breach involved the exposure of a wide range of sensitive information including names, addresses, social security numbers, driver’s license and passport details, claim information related to dental procedures and payment histories, health insurance policy numbers, tax identification numbers, and financial account details. The breach impacted nearly 7 million individuals encompassing customers of Delta Dental of California and affiliated entities.

If Delta Dental relied on legacy systems, they might have lacked modern security updates and patches, making them easy targets for cyberattacks. Sensitive data may not have been properly encrypted, allowing hackers to access information in its original form. If hackers gained access to one part of the network, they might have had free rein to access other areas due to a lack of proper segmentation. Ineffective real time monitoring and alerting systems could have delayed the detection of the breach allowing attackers to exfiltrate more data. The attackers gained unauthorized access to Delta Dental’s systems and extracted large amounts of data. The C10p group proceeded to list the stolen data on its dark web site for download, increasing the breach’s exposure. These vulnerabilities align with broader trends in the insurance industry, where increasing sophistication in cyberattacks challenges existing defenses.

Delta Dental initiated a comprehensive investigation to assess the scope of the breach concluding by July 6th, 2023. Affected parties were informed of the breach on December 14th, 2023, with detailed notifications sent to assist customers in understanding the risks and next steps. The company worked with law enforcement and cybersecurity firms to address the breach and prevent further exploitation. The MOVEit Software company implemented updates to address vulnerabilities in the MOVEit platform. Steps were taken to strengthen cybersecurity protocols, including employee training, regular security audits, and advanced threat detection tools.

Delta Dental provided access to free credit monitoring and identity theft protection services to mitigate customer risks. Customers were advised to remain vigilant for phishing attempts and monitor financial statements for suspicious activity. Delta Dental’s data breach is a reminder of the importance for companies to maintain robust cybersecurity measures for the protection of sensitive information. By addressing vulnerabilities and adopting proactive security strategies, organizations can reduce the likelihood of future incidents and build trust with their stakeholders.