INFO 6010 - S2023 Assignment 1

Gihan Shamike Liyanage

1142109

CISSP Prep

28/05/2023

## Toyota Admits Decade-Long Data Leak Affecting 2.15 Million Customers

Toyota Motor Corp. has acknowledged a decade-long leak of customer data affecting about 2.15 million customers in Japan starting in November 2013 and continuing through mid-April 2023, involving Toyota's cloud-based connected service, which reminds vehicle owners to maintain their vehicles. The information that has been compromised includes the vehicle's identification numbers, vehicle location history, and videos from the drive recorders. Although Toyota has stated that this data cannot be used to identify specific owners, it has affected 2.15 million customers of services including G-Link, G-Book, and Connected. The CEO and founder of the security software company X-Phy, Camellia Chan, emphasizes the potential dangers arising from human error within organizations. She points out that businesses frequently make it convenient for cybercriminals by inadequately configuring their networks. Furthermore, according to Mark Stockley, a senior threat researcher at Malwarebytes, the growing use of cloud and NoSQL data storage has led to incidences of exposed data. One of its representatives stated that the incident had been reported to Japan's Personal Information Protection Commission, but declined providing more information because it is customary for the commission to avoid commenting on specific instances.

According to Toyota, this data by itself cannot be utilized to identify specific owners. However, the impacted clients are still exposed to a number of possible threats. The leak exposed personal information, such as location history, which could invade the privacy of the affected customers. It may allow unauthorized people to track or monitor them. Even though Toyota asserts that the information cannot be used to identify specific people, there is still a possibility of data exploitation. In order to create comprehensive profiles of the impacted clients, cybercriminals may attempt to integrate this data with additional information. Apart from that, the affected clients are more likely to become victims of identity theft, frauds, and other cybercrimes as a result of this data leakage. Armed with this private information, thieves can use it to trick customers through impersonation or targeted phishing attacks. By using hacked data to create convincing messages or phone calls, they may deceive users into disclosing additional personal information or financial information. Besides, this data breach could seriously damage Toyota's reputation, causing customers to decrease confidence in the company's ability to keep their personal information secure. And this is not the first time Toyota has faced a data leak, which might make customers question how well Toyota is handling data security.

Toyota faces numerous difficulties as a result of the data breach, from possible financial and legal repercussions to reputational harm and issues with customer trust. In order to protect their data and keep customers confident, it highlights the significance of effective cybersecurity safeguards and data protection procedures for businesses. The company may experience legal and regulatory implications for the breach, depending on the applicable data protection regulations. This could lead to fines, penalties, or other legal measures. Other than that, the breach may strain the relationship between Toyota and its customers. It could result in customer dissatisfaction, increased customer support demands, and potential loss of business. Additionally, Toyota may suffer considerable financial losses as a result of dealing with the data breach, conducting investigations, putting security measures in place, and maybe compensating impacted customers. And also, it's possible that the breach will benefit rivals of Toyota. Customers who are concerned about data security might opt for different brands or services instead of Toyota, which would hurt the company's standing in the market.

Obtaining information through a data breach is a crime. Unauthorized access to computer systems, computer network, database, unauthorized disclosure of personal data, and unauthorized use of sensitive information are typically illegal activities in many jurisdictions. Specific laws and regulations regarding data breaches can vary from country to country. And also, if the obtained information is used for the purposes of theft, fraud, identity theft, or any other criminal activity, it is considered a crime. Many countries have data protection regulations in place that establish strict requirements on businesses to safeguard personal data. Legal repercussions may result from a data breach brought on by insufficient security precautions or a failure to adhere to these regulations.

To protect customer information and enhance data security from outsider attacks, Toyota should consider reviewing and implementing several measures like carrying out a comprehensive analysis of its security procedures and infrastructure. This entails putting in place strong firewalls, intrusion detection systems, encryption standards, and access controls. Other than that, implementing regular security audits and assessments can help identify vulnerabilities, address potential weaknesses, and ensure compliance with industry standards and best practices. Employee education in data security best practices is essential. This includes stressing the value of strong passwords, phishing awareness, and the responsible handling of sensitive data. Programs for regular training can reduce the possibility of neglect or human error. Furthermore, developing a comprehensive incident response plan enables Toyota to respond immediately and effectively to any future breaches. These strategies should include specific instructions for finding, preventing, and dealing with security incidents, as well as for informing consumers who may be impacted.

Other than that, protecting intellectual property from insider threats within an organization is also crucial. Implement strong access controls and user authentication mechanisms, provide comprehensive training to employees about the importance of intellectual property protection, Separation of Duties and Employee Exit Procedures are some measures that can be taken as an initial step. Additionally, Toyota should implement some security policies for employees, contractors, and third parties with access to intellectual property to sign confidentiality agreements or non-disclosure agreements (NDAs). These agreements legally bind individuals to maintain the confidentiality of sensitive information. Implementing robust monitoring and auditing systems to detect and track access and usage of intellectual property is also mandatory. Also regularly examining logs and audit trails plays a crucial role in preventing attacks by helping to identify any suspicious or unauthorized activities in a timely manner.

"There was a lack of active detection mechanisms, and activities to detect the presence or absence of things that became public," the company’s spokesperson provided an explanation for the delay in recognizing the error. In this situation, Toyota has already declared that it will implement a system to audit cloud configurations, set up a system to continuously monitor configurations, and properly train staff on data handling guidelines. As a summary, the incident involving Toyota Motor Corp highlights important lessons for organizations. Proper configuration of networks and cloud services, active detection mechanisms, data encryption, and anonymization are crucial. Regular security audits, employee training, and vendor management are essential. Prompt incident response and transparent communication are vital. The breach emphasizes the significance of ensuring data security and privacy. Organizations must prioritize robust security measures, implement monitoring systems, and conduct regular audits to identify vulnerabilities. Training employees in data handling and cultivating a culture of security awareness are crucial. Effective vendor management and adherence to security standards are essential to protect sensitive data.

# References

Komiya, D. L. (2023). *More than 2 million Toyota users face risk of vehicle data leak in Japan*. Retrieved from Reuters.com: https://www.reuters.com/business/autos-transportation/toyota-flags-possible-leak-more-than-2-mln-users-vehicle-data-japan-2023-05-12/

Mascellino, A. (2023, May). *Toyota Admits Decade-Long Data Leak Affecting 2.15 Million Customers*. Retrieved from Infosecurity-magazine.com: https://www.infosecurity-magazine.com/news/toyota-admits-decade-long-data-leak/