IDENTITYIQ®

CASE STUDY: THE NATIONAL RAILROAD CORP. (AMTRAK)

IdentityIQ.com
888-467-7102 Option 2
sales@idiqpartners.com

Case Study: The National Railroad Corp. (Amtrak)

Studies have shown there is a direct correlation between a business's planning and response to overall data breach costs. In fact, an organization can lower its data breach response costs by an average of $360,000 by having an incident response team that undergoes security awareness training and establishes a response plan prior to a data breach.*

One of the most recent data breach incidents that exemplify a prepared incident response to a data breach is with the case of the National Railroad Corp., otherwise known as Amtrak. The organization discovered a data breach with an unknown party gaining access to Amtrak Guest Rewards accounts with some personally identifiable information (PII) exposed.

Data Breach Vulnerability

This cyberattack comes only a year after Amtrak had already addressed major security flaws in its iOS application. The Amtrak mobile application gives users an Amtrak Guest Rewards account, which acts as a self-service kiosk, allowing users to save credit card information for quick check-outs, purchase e-tickets, manage their travel information and earn rewards.

The proactive cybersecurity consulting firm, Bishop Fox, noticed the vulnerability and found the security flaw involved two API endpoints in the app backend that failed to

enforce authentication that would grant an attacker access to customer data. Bishop Fox determined that if exploited the flaw could lead to a data breach of at least 6 million Amtrak Guest Reward accounts. The data at risk included PII such as full names, addresses, and phone numbers, along with partial payment data.

Furthermore, if passengers had any upcoming travel plans, all of their trip information along with partial payment data – including the last four digits of the credit card, expiration date and billing address – is at risk of exposure. If the user had entered their date of birth and citizenship information for the trip, that information would be vulnerable as well.

With access to a passenger's Amtrak Guest Rewards account, an attacker could effectively steal funds by canceling a trip and requesting a refund in the form of an eVoucher code that could legitimately be used on Amtrak's website. Although the app would attempt to verify ownership by requesting related PII, the refund request would inevitably be granted as the attacker would already have that information. With the e-voucher code in hand, anyone could successfully buy a new ticket. According to the cybersecurity company, the vulnerability was patched earlier last year.

Now fast forward one year later, and attackers manage to access Amtrak Guest Rewards accounts despite recent application patches. And how did Amtrak respond? With reactive security measures. The security team terminated the unauthorized data, reset passwords for the affected accounts and implemented additional safeguards to protect the identity of their customers.

Amtrak protected their customers by giving them access to a year of credit and identity monitoring, identity restoration and identity theft insurance up to $1 million to cover for legal fees, lost wages, and stolen funds.

Be Prepared for a Data Breach

In this incident, Amtrak showcased a balanced approach of proactive and reactive problem management. The organization first implemented preventative measures by performing an ethical hack on their own system in order to uncover vulnerabilities that required patching. Despite these updates, however, hackers still managed to find an entry point.

Amtrak proved their ability to handle the situation by quickly terminating the threat within a few hours and quickly proceeded to notify state officials and the customers who were affected by the breach. Additionally, Amtrak showed that the organization cared for its relationship with customers by incorporating them into the incident response plan. Customers received access to identity theft insurance in case their information was used maliciously.

The more organizations are prepared to deal with every stage of a data breach incident, the more the problem can be prevented or solved, saving money in the long-run.

As data breaches and their costs continue to rise over time, businesses of all sizes need to have a plan in place that includes preparation, monitoring and response support.*

About **IdentityIQ**

Offered by IDIQ®, IdentityIQ® services are the solution for credit report and identity theft monitoring. Our team of experts utilizes innovative techniques for active credit report monitoring and identity theft protection, so you have financial peace of mind. An industry leader, IdentityIQ services have been named to the Inc. 5000 list of the fastest-growing companies in the United States by "Inc." magazine and "50 Most Valuable Brands of the Year" by "The Silicon Review". For more information, visit IdentityIQ.com.

SOURCES:
Amtrak Notice of Data Breach
BishopFox Amtrak Mobile APIs - Multiple Vulnerabilities
IBM Security: Cost of a Data Breach 2019
For more information, visit idiq.com and identityiq.com.