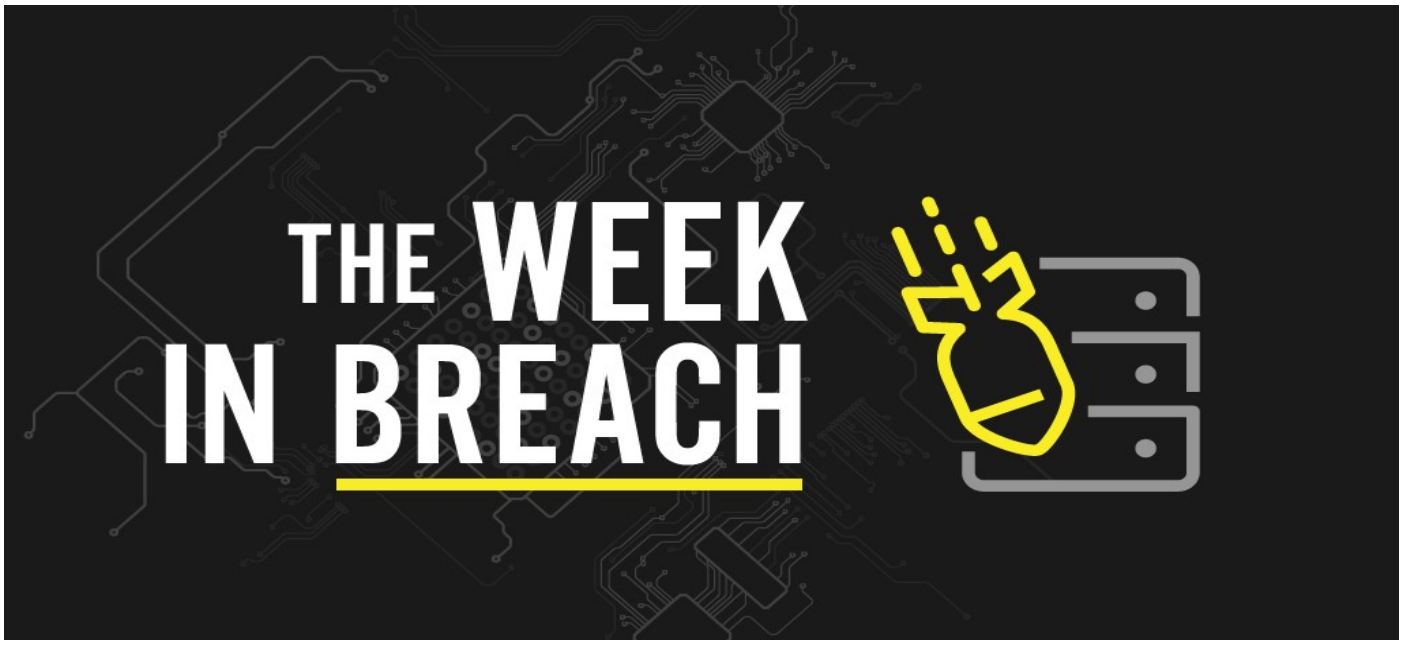
THE WEEK IN BREACH NEWS: 05/26/21—6/01/21

DenBe Computer Consulting
Connecting Business

June 2, 2021 by Dennis Jock

Cybercriminals pulled off a meaty breach at JBS SA, Canada Post is wrapped up in a third-party breach, how federal data breach and infrastructure risk reduction efforts might impact businesses and 5 webinars to help you harness new revenue streams!



If your business isn't using our ***Dark Web Monitoring Services*** please call us for a free scan and to discuss setting up this cutting edge monitoring service for you!

Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan.*** You will get a free, no obligation scan sent to your inbox within 24hrs. ***Visit today: www.denbeconsulting.com***

United States – DailyQuiz

https://therecord.media/8-3-million-plaintext-passwords-exposed-in-dailyquiz-data-breach/

Exploit: Hacking

DailyQuiz: Entertainment App

Risk to Business: **1.655= Severe**

The personal details of 13 million DailyQuiz users have been leaked online after a hacker breached the app developer's database. Millions of user passwords were stored in that database unsafely in a plain text format and were subsequently stolen. Researchers recently discovered that the DailyQuiz database was up for sale in dark web data markets.

Individual Risk: **2.711 = Moderate**

Users should be aware that their passwords have been compromised and change any accounts that share that password as well as updating their DailyQuiz accounts.

Customers Impacted: 13 Million

How It Could Affect Your Business: Weak password storage is symptomatic of low cybersecurity safety standards and shows clients that you don't take their data privacy seriously.

United States – Rehoboth McKinley Christian Health Care Services (RMCHCS)

https://portswigger.net/daily-swig/us-healthcare-non-profit-reports-data-breach-impacting-200-000-patients-employees

Exploit: Hacking

Rehoboth McKinley Christian Health Care Services (RMCHCS): Health Non-Profit

Risk to Business: **1.833= Severe**

Rehoboth McKinley Christian Health Care Services (RMCHCS) has reported a data breach reported caused by improper access to data impacting around 200,000 patients and employees. RMCHCS operates a 60-bed acute care hospital and four clinics providing emergency care, cancer care, and hospice and pediatric services in Arizona and New Mexico. The company did not say how the data was improperly accessed.

Risk to Business: **1.833= Severe**

RMCHCS states that the breached material includes names, dates of birth, postal addresses, telephone numbers, and email addresses, as well as Social Security, driver's license, passport and (for Native Americans) tribal ID numbers. Healthcare-specific details of patient care were also involved, but it's not consistent across accounts. Healthcare data potentially impacted may include medical record numbers, dates of service and healthcare provider names; prescription, treatment, and diagnosis information; and billing and claims information, including financial account information.

Customers Impacted: 200,000

How it Could Affect Your Business: Data theft is always a problem, but theft of medical data is a disaster for healthcare orgs that will have to pay major fines for security failures.

United States – Bose

https://www.hackread.com/logistics-giant-leaks-data-lolz-when-alerted/

Exploit: Ransomware

Bose: Audio Equipment Maker

Risk to Business: 2.812 = Moderate

Audio manufacturing titan Bose disclosed a data breach following a ransomware attack that hit the company's systems in early March. In a regulatory filing, the company explained that a small amount of employee data had been potentially exposed as had several unnamed spreadsheets. No customer or other proprietary data was reported as compromised but the investigation is still ongoing.

Individual Risk: 2.812= Moderate

According to the company, a very small amount of employee personally identifying data and payroll data was compromised. Current and former employees should be alert to spear phishing and identity theft.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is evolving, meaning every incident stands a chance of containing an even harder to stop new variant that could do lasting damage.

Canada - Canada Post

https://globalnews.ca/news/7894760/canada-post-data-breach/

Exploit: Third Party Data Breach

Canada Post: Postal Service

Risk to Business: **1.882 = Severe**

A supplier's malware attack is responsible for a nasty data breach at Canada Post affecting 44 of the company's large business clients and their 950,000 receiving customers. The exposure comes from Commport Communications, an electronic data interchange (EDI) solution supplier that manages shipping data for business customers, informed Canada Post that address data associated with some of their customers had been compromised in May 2021. Canada Post has announced that only shipping information pertaining to less than 50 corporate customers was involved.

Individual Impact: No sensitive personal or financial information has been declared compromised in this incident and the investigation is ongoing.

Customers Impacted: 44 companies and an estimated 950,000 individual addresses

How it Could Affect Your Business: Third-party and supply chain data breaches like this one are becoming all too common as clever cybercriminals go for data-rich targets – and the problem will only get worse thanks to booming dark web data markets.

United States - JBS SA

https://www.hackread.com/uk-recruitment-firm-exposed-applicants-data/

Exploit: Ransomware

JBS SA: Meat Processor

Risk to Business: 1.221 = Extreme

International meat supplier JBS SA has been hit by a ransomware attack. The world's largest meat producer, Brazil-based JBS has operations in 15 countries and serves customers worldwide including the US, Australia and Canada. The company is in contact with federal officials and has brought in a "top firm" to investigate and remediate the incident which is potentially tied to nation-state cybercrime. JBS stated that the attack only impacts some supplier transactions and no data was stolen.

Individual Impact: No sensitive personal or financial information was reported as compromised in this incident and the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is the preferred weapon of cybercriminals, especially of the nation-state variety, for its potential for business disruption without even stealing data.

Australia - TPG Telecom

https://www.zdnet.com/article/a-pair-of-tpg-trustedcloud-customers-were-breached/

Exploit: Hacking

TPG Telecom: Communications Technology

Risk to Business: **1.115 = Extreme**

TPG Telecom has announced that it had the data of two unnamed large customers improperly accessed on its legacy TrustedCloud hosting service. It added it did not believe any other customers were impacted by the breach. The service was part of a 2011 acquisition by the telecom and is set to be decommissioned in August 2021. An investigation is underway and authorities have been informed.

Individual Impact: At this time, no sensitive personal or financial information was announced as compromised in this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Attacks on older systems are often easy money for cybercriminals looking for data to sell with a low overhead and fast turnaround time.

Japan - Net Marketing Co.

https://www.japantimes.co.jp/news/2021/05/22/business/tech/omiai-dating-app-hack-japan/

Exploit: Hacking

Net Marketing Co: App Creator

Risk to Business: **1.922 = Severe**

Japanese app company Net Marketing Co. said Friday that the personal data of 1.71 million users of one of its apps has been compromised in a hacking incident. The company is the operator of the popular dating app Omiai. Net Marketing said that Omiai customer information provided to the company between January 2018 and last month has been accessed on more than one occasion by unauthorized parties and PII on users may have been stolen.

Individual Risk: **1.942 = Severe**

The company notes that assorted user data, including names, identity cards, addresses, email addresses and face photos, was likely leaked due to unauthorized access to its server. Customers that use the Omiai app should be cautious for spear phishing and identity theft risk.

Customers Impacted: Unknown

How it Could Affect Your Business: Personal data like this is a hot commodity in booming dark web data markets. Failing to protect it adequately makes it catnip for cybercriminals.

India - Air India

https://www.bleepingcomputer.com/news/security/air-india-data-breach-impacts-45-million-customers/

Exploit: Third Party Data Breach

Toshiba: Electronics Manufacturer

Risk to Business: **2.001 = Severe**

Air India disclosed a data breach impacting 4.5 million of its customers following the hack of airline passenger service system provider SITA in February 2021. Dozens of airlines around the world had data exposed in that ransomware incident and the fallout is still shaking out. The airline confirmed that the breach involved personal data and credit card information registered between August 2011 and February 2021 by Air India or its subsidiaries.

Risk to Business: **2.113 = Severe**

The exposed data is reported to include passenger details like name, date of birth, contact information, passport information, ticket information, Star Alliance, and Air India frequent flyer data as well as credit card numbers.

Customers Impacted: Unknown

How it Could Affect Your Business: Third-party and supply chain data breaches like this one are becoming all too common as clever cybercriminals go for data-rich targets – and the problem will only get worse thanks to booming dark web data markets.

India - Domino's Pizza India

https://ciso.economictimes.indiatimes.com/news/user-info-linked-to-18cr-dominos-orders-leaked/82899181

Exploit: Hacking

Domino's Pizza India: Restaurant Chain

Risk to Business: 1.774 = Severe

Customer and employee information has been exposed in a hacking incident at Domino's Pizza India. Security researchers discovered 13TB of employee files and customer details exposed on the dark web. The data leak may be connected to another breach of the pizza chain earlier in April. Jubilant FoodWorks, operator of the chain, said that customers' financial information remains safe.

Risk to Business: 1.671 = Severe

It is unclear what if any payment data was snatched, but personal information for customers including order dates, addresses, names, order invoices and similar data is available. The hackers claim to also have employee data, but that is unconfirmed.

Customers Impacted: 180 million

How it Could Affect Your Customers' Business: Personal data is the most desirable information for cybercriminals right now, and every company needs to take precautions to keep them out of databases.

Japan—Mercari

https://www.bleepingcomputer.com/news/security/e-commerce-giant-suffers-major-data-breach-in-codecov-incident/

Exploit: Supply Chain Data Breach

Mercari: E-commerce Platform

Risk to Business: 1.922 = Severe

In another big supply chain hit this week, Japanese marketplace Mercari has been compromised as a result of the recent Codecov breach. earlier this year, code coverage tool Codecov disclosed that it had been a victim of a supply-chain attack that lasted for two months and allowed cybercriminals to meddle with its popular Bash Uploader, opening hundreds of companies up to risk. Mercari announced that tens of thousands of customer records, including financial information, were exposed to external actors due to the Codecov breach.

Individual Risk: 1.942 = Severe

In the final tally, 17,085 records related to the transfer of sales proceeds to customer accounts were exposed including bank code, branch code, account number, account holder (kana) and transfer amount; 7,966 records on business partners of “Mercari” and “Merpay,” including names, date of birth, affiliation, e-mail address, and other data were exposed. 2,615 records on employees were also impacted including those working for a Mercari subsidiary. The data is comprised of names of some employees as of April 2021, company email address, employee ID, telephone number, date of birth and other PII plus details of past employees, some contractors and employees of external companies who interacted with Mercari.

Customers Impacted: Unknown

How it Could Affect Your Business: Third-party data breaches like this one are the future of business. Reliance on outsourced service providers gives cybercriminals an easy way to scoop up data or snatch access credentials for multiple targets in one fell swoop.