THE WEEK IN BREACH NEWS: 10/21/20 – 10/27/20

DenBe Computer Consulting
Connecting Business

October 28, 2020 by Dennis Jock

This Week in Breach News: Pharmaceutical companies have a tough week with hacking as manufacturing is disrupted at COVID-19 drug makers and huge patient databases are exposed, and why selling access for profit is on the rise.

The Week in Breach News: Top Threats This Week

- **Top Source Hits:** ID Theft Forum
- **Top Compromise Type:** Domain
- **Top Industry:** Education & Research
- **Top Employee Count:** 1-10

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***

Maxex

https://www.inforisktoday.com/blogs/home-loan-trading-platform-exposes-mortgage-documentation-p-2959

Exploit: Unsecured Database

MAXEX: Loan Trading

Risk to Business: 1.772 = Severe

Georgia-based home loan trader MAXEX had a data disaster this week as an estimated 9GB of data leaked from a suspected insecure server. Some of the data is from backend software development for its loan-trading platform. But a substantial portion included confidential banking documents, system login credentials, emails, the company's data breach incident response policy, and cybersecurity readiness reports. The breach also exposed complete mortgage documentation for at least 23 individuals in New Jersey and Pennsylvania. The incident investigation is ongoing.

Individual Risk: 2.011 = Severe

Financial information for clients was leaked, opening customers up to identity theft concerns. Some impacted clients had no idea that MAXEX currently had their loan, creating complications for informing customers who may be affected. Consumers should check to see who is servicing their mortgage and take precautions against identity theft and spear phishing if that provider is MAXEX.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Sloppy security can mean that if you do have an incident like a data breach, you might not even know where to start looking for the cause, putting your business at risk for an expensive investigation in addition to a data disaster.

Made in Oregon

https://www.infosecurity-magazine.com/news/oregon-retailer-suffers-sustained/

Exploit: Unauthorized Database Access

Made in Oregon: Specialty Gift Retailer

Risk to Business: 1.669= Severe

Customers of gift retailer Made in Oregon got a little something extra when they purchased their treats – a side order of fraud. For more than 6 months, cybercriminals gained access to its e-commerce site, stealing payment information for transactions that occurred between the first week of February 2020 and the last week of August 2020.

Individual Risk 1.669 = Severe

Customers who made an online purchase from Made in Oregon may have had their name, billing address, shipping address, email address, and credit card information compromised. The company has sent out notices to people who could be impacted, warning of identity theft and spear phishing dangers.

Customers Impacted: 7,800

How it Could Affect Your Customers' Business: Information that is stolen in incidents like this often ends up on the Dark Web in a data dump or information market where it powers cybercrime for years to come.

Pfizer

https://pharmafield.co.uk/pharma_news/pfizer-suffers-huge-data-breach-on-unsecured-cloud-storage/

Exploit: Unsecured Database

Made in Oregon: Drugmaker

Risk to Business: **1.401 = Extreme**

In a monster week for pharma hacking, Pfizer leads the pack with a substantial data breach that it brought on itself. In a huge blunder, unsecured and unencrypted data containing logs, transcripts, and details of patient helpline conversations was leaked from a misconfigured Google Cloud storage bucket. The exposed data included detailed information regarding hundreds of conversations between Pfizer's automated customer support software and patients using drugs including Lyrica, Chantix, Viagra, Ibrance, and Aromasin.

Individual Risk **1.412 = Extreme**

The exposed call or chat transcripts had extensive PII and medical data for patients including full names, addresses, phone numbers, and details of health and medical conditions. The transcripts also contained detailed information about treatments, patient experiences, and questions related to products manufactured and sold by Pfizer.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Leaving this kind of information laying around is a hacker's dream, and a security nightmare for your business as not only the recovery costs but the regulatory penalties for exposing this kind of data adds up.

City of Shafter

https://bakersfieldnow.com/news/local/city-of-shafter-hit-by-ransomware-attack

Exploit: Ransomware

City of Shafter: Municipal Government

Risk to Business: 1.714 = Severe

Cyberattacks against city governments and municipal services have been climbing worldwide, and Shafter, CA just joined the list after a ransomware attack took it's systems offline for several days. The attack impaired the operations and delivery of city services, a common hallmark of recent municipal cybercrime.

Individual Risk: No personal or consumer information was reported as impacted in this incident.

Customers Impacted: 20,000

How it Could Affect Your Customers' Business: Ransomware has been a menace to municipal governments large and small. Just last week, the Hackney Borough Council in London was rocked by ransomware, and the risk is growing for governments as incidents pile up.