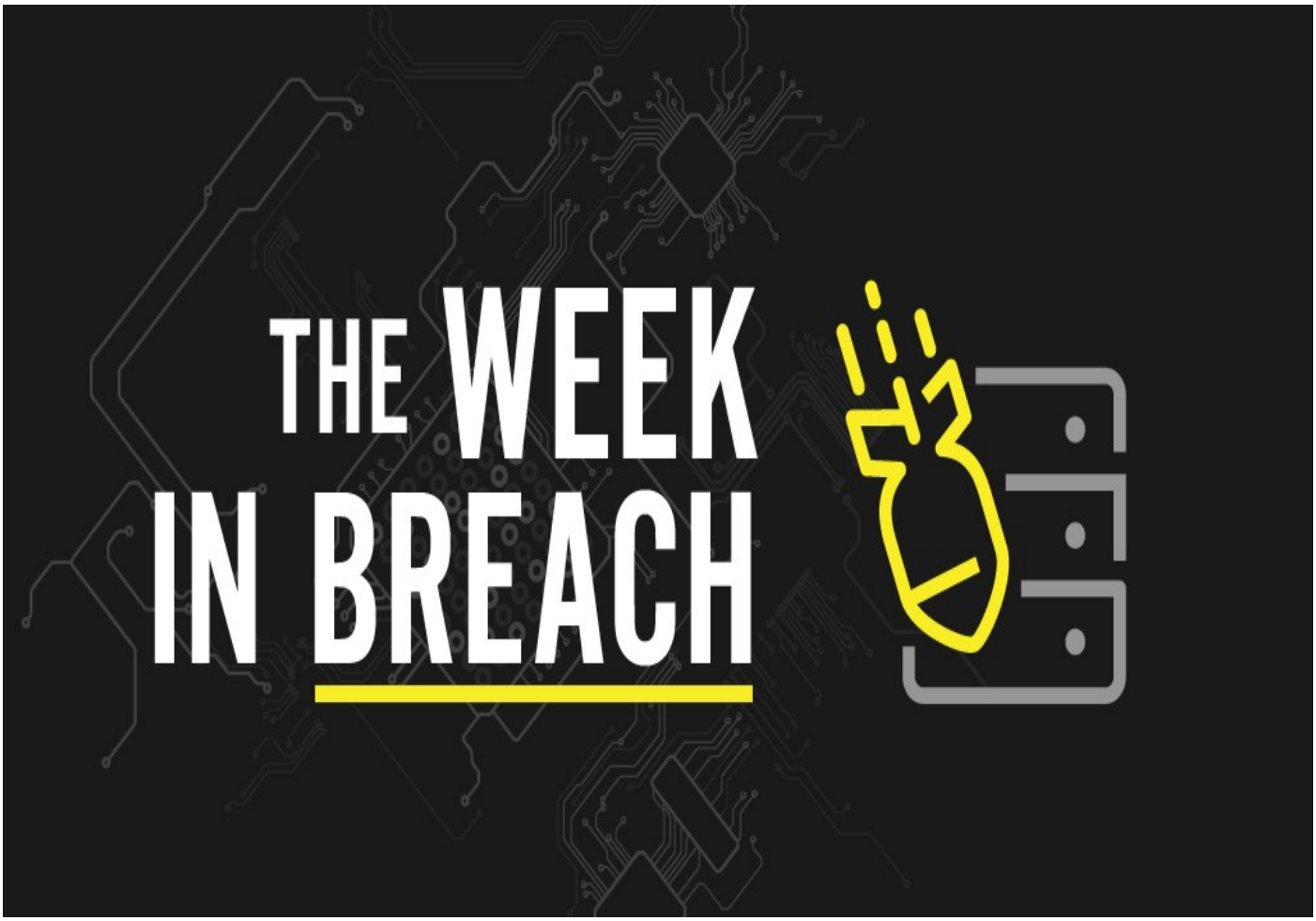
# THE WEEK IN BREACH NEWS: 07/26/22– 08/03/22

DenBe Computer Consulting
Connecting Business

August 3rd by Dennis Jock




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***

Twitter
https://www.bleepingcomputer.com/news/security/hacker-selling-twitter-account-data-of-54-million-users-for-30k/

**Exploit**: Hacking

Twitter: Social Media Network

**Risk to Business: 2.783 = Moderate**

Cybercriminals say that they've exploited a vulnerability in the Twitter platform to obtain data about 5.4 million accounts. Altogether, bad actors claim to have snatched data from 5.4 million accounts, with the data now up for sale on a hacker forum for $30,000. Twitter was alerted to the exploit in January 2022 and fixed it quickly, but the damage had already been done. The method used to scrape the data was similar to an attack on Facebook in 2021. Twitter has not confirmed or denied the attack as of press time, saying that the incident is under investigation.

**Individual Impact:** No information about consumer/employee PII, PHI or financial data exposure was available at press time.

AllOne Health Resources, INC.
https://www.jdsupra.com/legalnews/allone-health-resources-inc-discovers-8173610/

**Exploit:** Business Email Compromise (BEC)

AllOne Health Resources: Insurance Company

**Risk to Business: 1.672 = Severe**

AllOne Health Resources, Inc. Has experienced a data breach as the result of a business email compromise attack. The company says that an unauthorized party gained access to sensitive consumer data contained on its network after landing the BEC attack. According to AllOne Health, the company discovered the breach after it realized that the company's finance department had sent several wire transfers to a fraudulently created bank account. That prompted an investigation which revealed that bad actors had gained access to an employee's email account and snatched sensitive data.

**Individual Risk: 1.703 = Severe**

Exposed information includes the names, addresses, dates of birth, driver's license numbers, Social Security numbers and health information of 13,669 individuals.

**How it Could Affect Your Business:** A data security disaster in the healthcare sector is extra expensive and damaging after regulators weigh in.

## Blue Cross and Blue Shield (BCBS) of Massachusetts

https://healthitsecurity.com/news/bcbs-of-massachusetts-reports-third-party-vendor-data-breach

**Exploit**: Supply Chain Risk

Blue Cross and Blue Shield (BCBS) of Massachusetts: Insurance Company

**Risk to Business: 1.701 = Severe**

Blue Cross and Blue Shield (BCBS) of Massachusetts has filed a notice with the Maine Attorney General's Office stating that the company had suffered a breach of employee pension data thanks to an insider incident at a vendor, LifeWorks US. BCBS of Massachusetts and BCBS of Massachusetts HMO Blue used the vendor for services related to employee pension plan payments. BCBS says that on May 17, 2022, a now former LifeWorks employee mishandled data by emailing spreadsheets containing identifiable information about BCBS employees to both their personal email address and the personal email address of another

**Individual Impact:** No information about consumer/employee PII, PHI or financial data exposure was available at press time.

**How It Could Affect Your Business:** Supply chain risk is an ongoing problem that won't be going away anytime soon, and cybercrime doesn't even have to be involved for it to damage a business.

Entrust
https://www.bleepingcomputer.com/news/security/digital-security-giant-entrust-breached-by-ransomware-gang/

**Exploit**: Ransomware

Entrust: Software Company

**Risk to Business: 1.776 = Severe**

Digital security software maker Entrust has confirmed that it suffered a cyberattack where threat actors breached its network and stole data from internal systems. Entrust says that about two weeks ago, bad actors penetrated security and gained access to corporate data. The company maintains that data theft does not have an impact on its products and services. No ransomware group has claimed responsibility for the attack as of press time, and no ransom demand has been released.

**Individual Impact:** No information about consumer/employee PII, PHI or financial data exposure was available at press time.

**How it Could Affect Your Business:** Bad actors aren't just looking for PII/PHI or financial data, they're also in the market to steal data about OT and proprietary data.

Neopets
https://www.bleepingcomputer.com/news/security/neopets-data-breach-exposes-personal-data-of-69-million-members/

**Exploit:** Hacking

Neopets: Video Game Website

**Risk to Business: 2.304 = Severe**

Virtual pet website Neopets has suffered a data breach that resulted in the theft of source code and a database containing the personal information of over 69 million members. A hacker on the dark web going by the name TarTarX is selling the source code and database for the Neopets.com website for four bitcoins. Neopets recently launched NFTs that will be an element in an upcoming online Metaverse game.

**Individual Risk: 2.215 = Severe**

The data includes members' usernames, names, email addresses, zip code, date of birth, gender, country, an initial registration email and other site/game-related information.

**How it Could Affect Your Business:** The bad guys are always hungry for big pools of data, and adding some source code to the mix makes it even better.

Gas South, LLC
https://www.securityweek.com/glass-and-metal-packaging-giant-ardagh-group-discloses-cyberattack

**Exploit**: Hacking

Gas South, LLC.: Natural Gas Company

**Risk to Business: 1.929 = Severe**

Atlanta, Georgia natural gas provider Gas South has disclosed a data breach that may have exposed consumer data. The company says that an unauthorized party had access to its network between February 13 and February 23, 2022, with access to sensitive consumer data related to 38,000 individuals. Gas South is the largest natural gas provider in the Southeastern United States.

**Individual Risk: 2.215 = Severe**

The consumer information exposed may have included customers' Social Security numbers, driver's license numbers and financial data.

**How it Could Affect Your Business:** Utilities and other infrastructure targets have been under the gun for the last year, with 14 of 16 critical infrastructure sectors hit by a cyberattack in 2021.