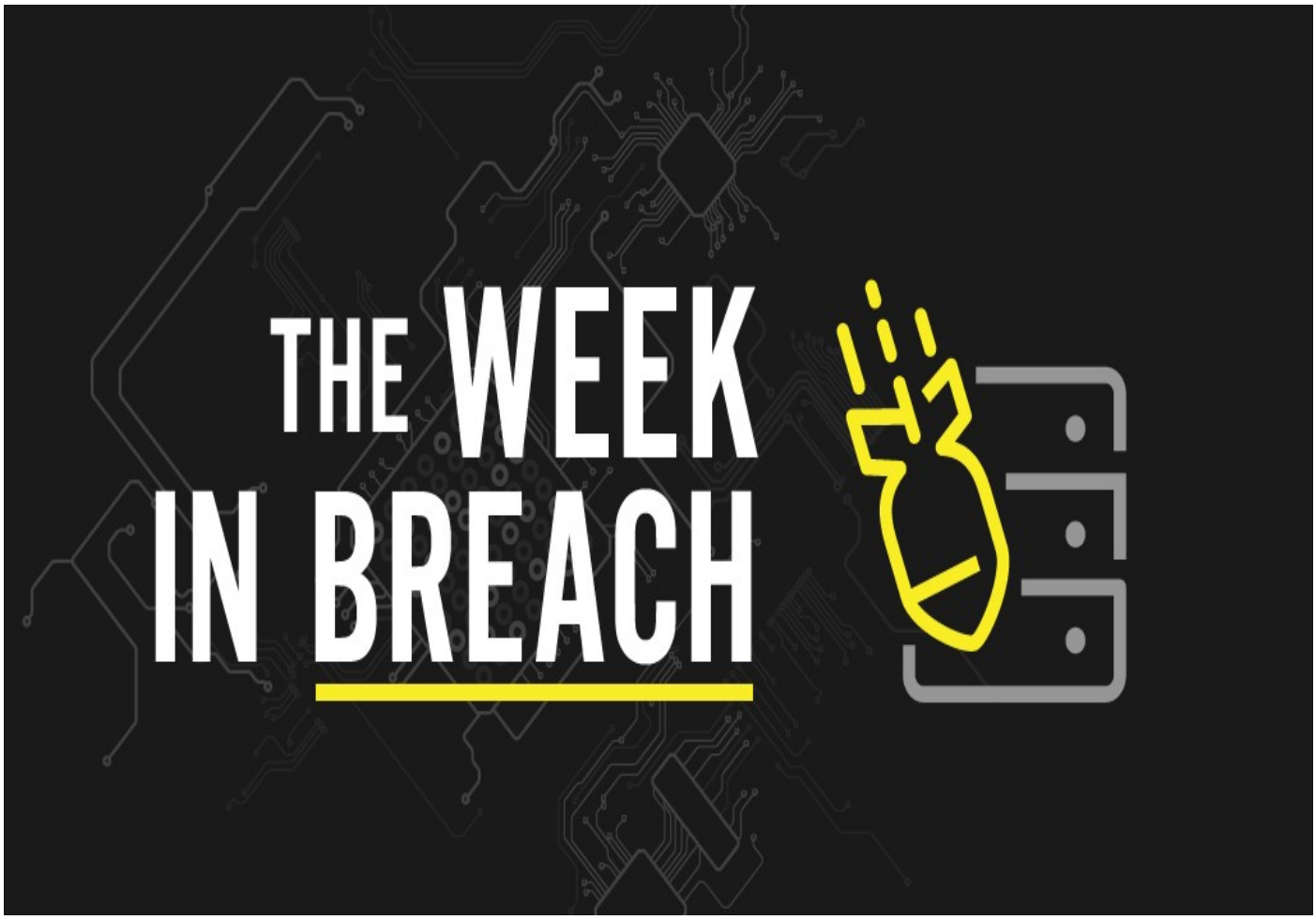
The Week in Breach News: 01/26/22 – 02/01/22

DenBe Computer Consulting
Connecting Business

February 02, 2022 by Dennis Jock



International tensions ratchet up nation-state cybercrime fears in a spate of incidents, another rough week for De Fi and 6 points to use when selling your clients on security awareness training.

Advocates

https://www.scmagazine.com/analysis/breach/68k-affected-by-data-theft-sophisticated-network-hack-of-nonprofit-advocates

Exploit: Hacking

Advocates: Health & Social Services Non-Profit

to Business: 1.727= Severe

Advocates announced that it had been the victim of a cyberattack. A hacker gained access to the organization's network in mid-September 2021. The attacker gained access to data tied to 68,000 clients served by Advocates and likely copied the data. The Massachusetts-based non-profit provides a range of services for individuals with autism, brain injuries, mental health, addiction, and other health conditions. Advocates is cooperating with the ongoing FBI investigation.

Individual Risk: 1.603= Severe

Current and former clients of Advocates are at risk of having their data exposed in this incident. The stolen data included names, contacts, Social Security numbers, dates of birth, client identification numbers, health insurance information, diagnoses and treatments. All

Customers Impacted: 68,000

How It Could Affect Your Business *Companies that store large quantities of personal or medical information are prime targets for the bad guys.*

Senate of Puerto Rico

https://abcnews.go.com/International/wireStory/official-puerto-ricos-senate-targeted-cyberattack-82495236

Exploit: Hacking

Senate of Puerto Rico: State Legislative Body

Risk to Business: 2.223 =Severe

Puerto Rico's Senate announced Wednesday that it was the target of a cyberattack that disabled its internet provider, phone system and official online page Senate President José Luis Dalmau said in a statement that there is no evidence that hackers were able to access sensitive information belonging to employees, contractors or consultants, although the incident is still under investigation.

Individual Impact: No specifics about consumer/employee PII or financial data loss were available at press time.

Customers Impacted: Unknown

How It Could Affect Your Business: *A recent rash of ransomware attacks against media and communications organizations should have everyone in that sector on notice.*

Kings County Public Health Department

https://portswigger.net/daily-swig/california-public-office-admits-covid-19-healthcare-data-breach

Exploit: Misconfiguration

Kings County California Public Health Department: Local Government Agency

Risk to Business: 2.711= Moderate

Kings County, California announced that the security flaw in its public webserver made limited information on COVID-19 cases available on the internet. The misconfiguration has been chalked up to a negligent third-party contractor. Discovered in mid-November 2021, officials say that the flaw was in place starting on February 15, 2021, and was corrected on December 6, 2021.

Individual Risk: 2.701= Moderate

In a statement, the county said that names, dates of birth, addresses and COVID-related health information for county COVID-19 cases was among the data that was available to view. They've set up a dedicated call center to answer questions from the public.

Customers Impacted: Unknown

How It Could Affect Your Business *Misconfiguration incidents due to employee or contractor negligence are just as expensive and damaging as cybercrime when regulators get finished with companies that have them.*