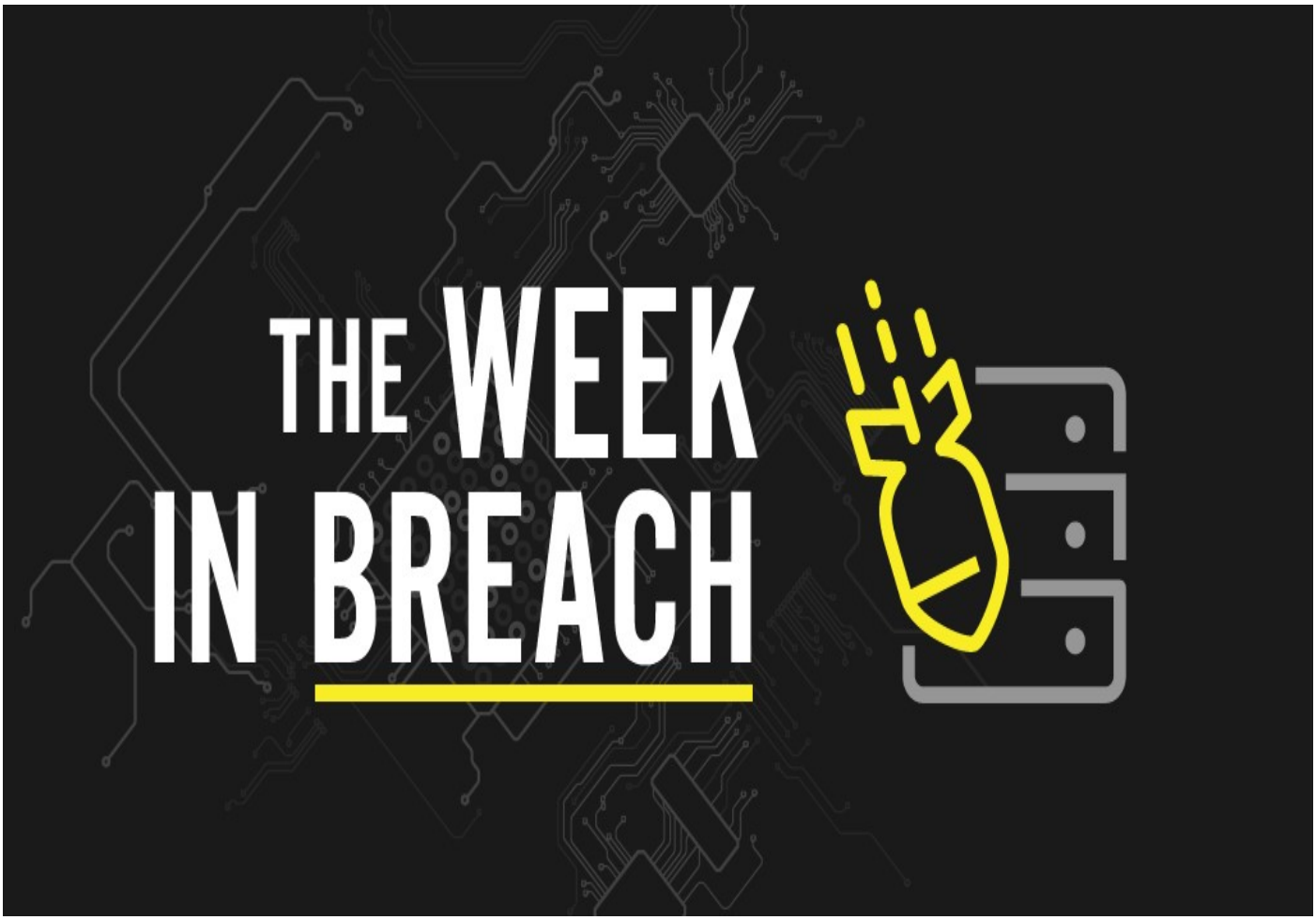
THE WEEK IN BREACH NEWS: 11/23/22 - 11/29/2022

DenBe Computer Consulting
Connecting Business

November 30th, 2022 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***

CorrectCare Integrated Health
https://www.jdsupra.com/legalnews/correctcare-integrated-health-announces-1605263/

Exploit: Misconfiguration

CorrectCare Integrated Health: Healthcare Provide

Risk to Business: 1.214 = Extreme

CorrectCare Integrated Health, a Kentucky-based company that specializes in providing healthcare to prisoners in U.S. jails, has experienced a data breach. In a filing with the California Attorney General's Office, the company stated that two file directories on the company's server had been accidentally exposed on the internet by an employee's misconfiguration of a server. An estimated 600,000 patients who received medical care in a CDCR facility between January 1, 2012, and July 6, 2022, were among those whose data was potentially impacted.

Risk to Business: 1.227 = Extreme

The breached information may include an individual's full name, date of birth, social security number, CDCR number and protected health information.

How it Could Affect Your Business: This employee mistake will cost the a fortune by the time regulators get finished with it.

Middletown Valley Bank
https://www.jdsupra.com/legalnews/middletown-valley-bank-reports-data-6177965/

Exploit: Hacking

Middletown Valley Bank: Financial Institution

Risk to Business: 2.177 = Severe

Maryland-based regional financial institution Middletown Valley Bank has disclosed that it has experienced a data breach as the result of an unspecified hacking incident. Around October 1, 2022, Middletown Valley Bank learned of a potential data security incident that resulted in the bank shutting down parts of its computer network. An investigation determined that an unauthorized party had gained access to its computer network. The unauthorized party was able to access files that contained sensitive information related to bank customers.

Risk to Business: 2.201 = Severe

The breached information varies depending on the individual and may include a customer's name, financial account numbers, Social Security number, driver's license number, passport number, and other information provided to the bank for purposes of applying for products or services.

How it Could Affect Your Business: The Banking and Finance sector was the top sector for ransomware attacks two years in a row, and the pace is not decreasing.