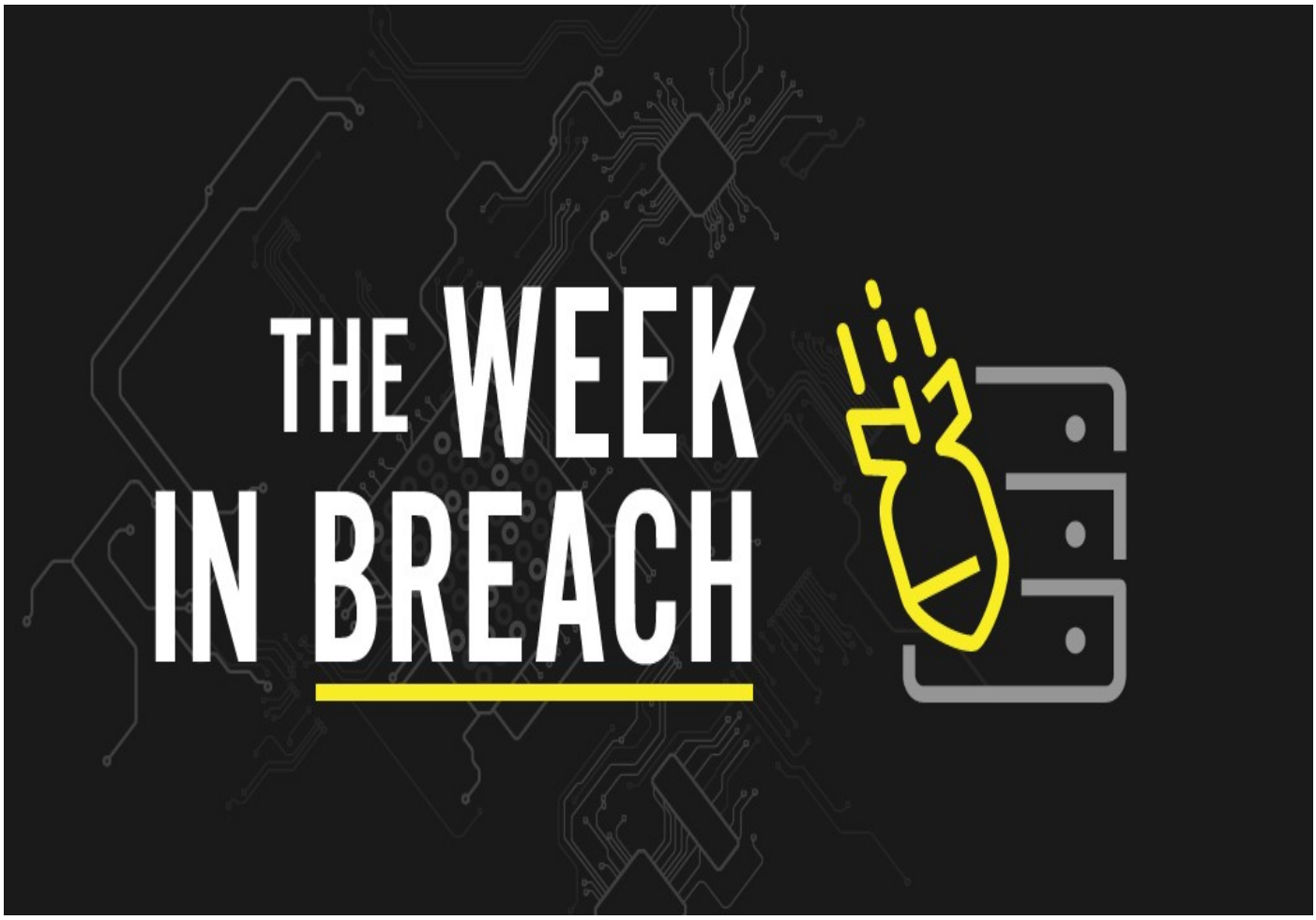
THE WEEK IN BREACH NEWS: 01/12/22 - 01/18/22

DenBe Computer Consulting
Connecting Business

January 19th, 2022 by Dennis Jock



Cybercriminals are snatching up financial data, bad actors rain on Parasol's parade.

Medical Review Institute of America (MRIoA)

https://www.securityweek.com/mrioa-discloses-data-breach-affecting-134000-people

Exploit: Ransomware

Medical Review Institute of America (MRIoA): Medical Analytics

Risk to Business: 1.227= Severe

Utah-based medical information and analysis company Medical Review Institute of America (MRIoA) announced that it has experienced a data breach. The incident was discovered on November 9, 2021, and officials were able to confirm that data had been stolen by November 16, 2021. In a data breach filing, the company said that over 134,000 individuals were impacted by the incident which is still under investigation. The company did say that it "retrieved and subsequently confirmed the deletion of" stolen data, but no information was released about a ransom amount or if they paid the ransom.

Risk to Business: 1.801= Severe

Protected health information was snatched including patients' names, gender, physical and email addresses, phone numbers, birth dates, Social Security numbers, full clinical information (including diagnosis, treatment, medical history, and lab test results) and financial information (such as health insurance policy and group plan

Customers Impacted: Unknown

How It Could Affect Your Business: *Ransomware risk is rising for organizations in every sector, especially companies that provide important services for other businesses.*

The Metropolitan Detention Center (MDC)

https://www.techtimes.com/articles/270004/20220103/hospital-data-breach-personal-info-1-3-million-patients-staff-data-breach.htm

Exploit: Ransomware

The Metropolitan Detention Center (MDC): Prison

Risk to Business: 2.223 =Severe

New Mexico prison officials had a problem on their hands as a ransomware attack impacted county computer systems resulting in a lockdown of the Metropolitan Detention Center (MDC) in Bernalillo County, New Mexico. The prison was not directly targeted. Inmates were forced to stay in their cells since the attack impacted the facility's security camera networks, automated doors and internet service. Inmates and jailors were also unable to videoconference for trials. Reports say that a number of databases are suspected of being compromised or corrupted including an incident tracker which records

Risk to Business: 2.419=Severe

The exposed personal data for patients and former patients at Broward health may include Social Security numbers, bank or financial account information, driver's license numbers, names, addresses, telephone numbers and hospital payment account information. Protected health information including medical information

Customers Impacted: Unknown

How It Could Affect Your Business *:Ransomware can cause serious operational problems in unexpected places in today's connected world.*

Illuminate Education

https://nypost.com/2022/01/15/nyc-schools-crippled-by-illuminate-educations-data-outage/

Exploit: Hacking

Illuminate Education: Education Platform

Risk to Business: 1.717= Severe

Illuminate Education, a digital education platform used by 5,200 schools and districts in the US, is still struggling to resume services after a cyberattack. The company owns popular school management platforms Skedula and PupilPath. Illuminate Education says it has continued experiencing a service interruption affecting all IO Classroom applications for nearly 10 days following an unspecified security incident. Investigation and recovery are underway, but the platform has not provided a recent update on the expected timeline.

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

Customers Impacted: Unknown

How It Could Affect Your Business *Cybercriminals have been all over targets in the education sector including companies that serve it. Companies should use caution.*

TransCredit

https://www.websiteplanet.com/blog/transcredit-leak-report/

Exploit: Misconfiguration

TransCredit: Credit Analysis & Reporting

Risk to Business: 1.719 = Severe

Over half a million credit reports and other financial documents held by Florida-based financial analysis firm TransCredit have been exposed. The Website Planet research team reported discovering a non-password-protected database that contained 822,789 records. Researchers cautioned that this dataset appears to be concentrated on clients in the transportation sector.

Risk to Business: 1.719 = Severe

The exposed data includes detailed information on trucking, transport companies and individual drivers. Also included in this data was information about credit accounts, loans, repayment and debt collections as well as financial data like banking information, tax ID

Customers Impacted: Unknown

How it Could Affect Your Business *Once again, a service provider that maintains a large array of records full of PII was hit, gaining cybercriminals a data bonanza.*