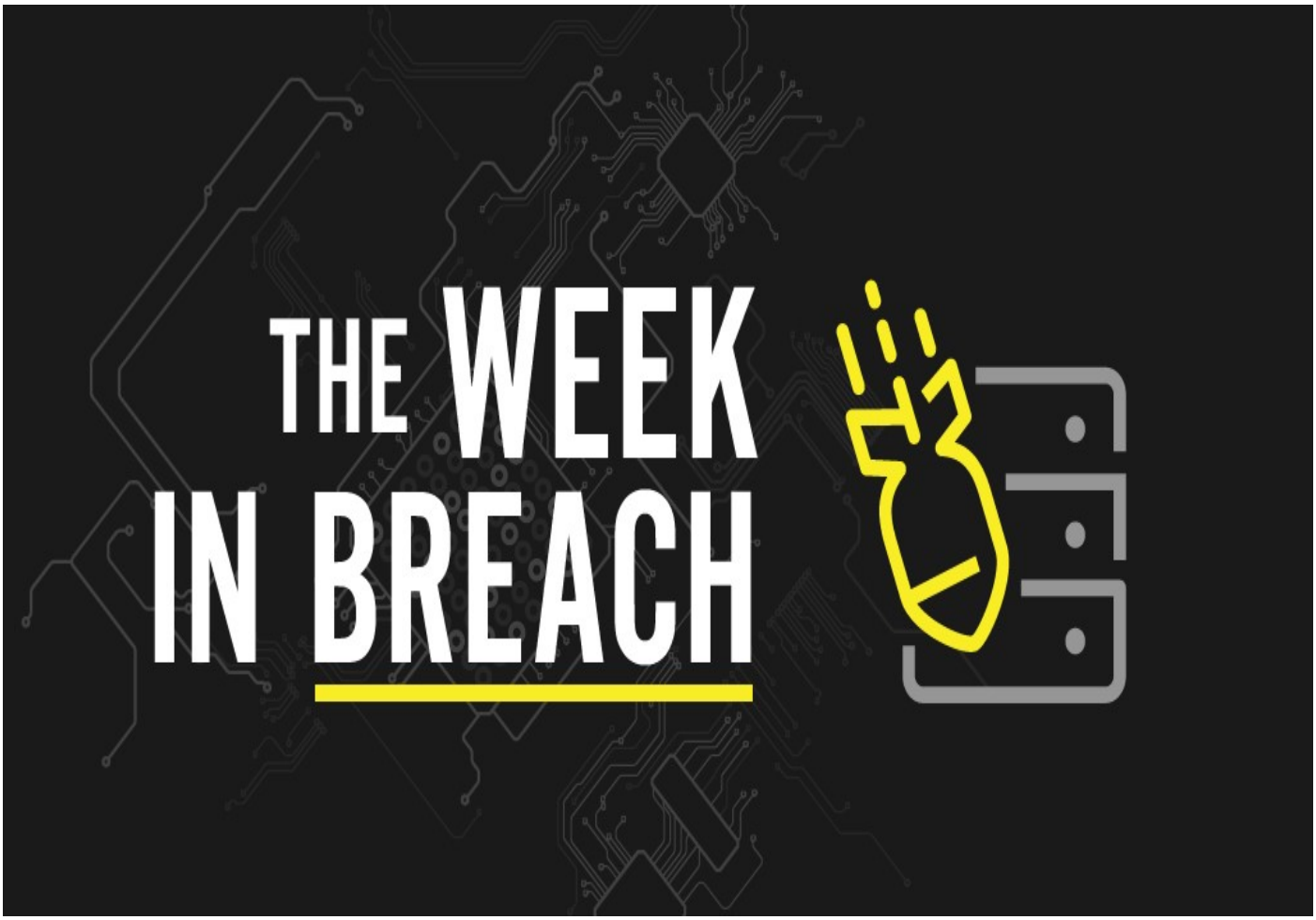
THE WEEK IN BREACH NEWS: 01/04/23 - 01/10/23

DenBe Computer Consulting
Connecting Business

January 11th, 2023 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***

The Housing Authority of the City of Los Angeles (HACLA)

https://therecord.media/los-angeles-housing-authority-says-cyberattack-disrupting-systems/

Exploit: Ransomware

The Housing Authority of the City of Los Angeles (HACLA): Municipal Government

Risk to Business: 2.176 = Severe

The Housing Authority of the City of Los Angeles (HACLA) has been hit by a cyberattack that is impacting its data security. HACLA appeared on the dark web leak site operated by the LockBit ransomware group last week. Reports say that on December 31, 2022, the LockBit ransomware group claimed that it had stolen 15 TB of data. The group also gave HACLA a deadline of January 12, 2023, to pay an undisclosed ransom. No specifics were available at press time about exactly what types of data were stolen or who that data may have belonged to.

How It Could Affect Your Business: This database could contain many kinds of privileged information and its loss will incur a heavy fine from data protection regulators.

Avem Health Partners
https://www.bankinfosecurity.com/hack-on-services-firms-vendor-affects-271000-patients-a-20755

Exploit: Supply Chain Attack

Avem Health Partners: IT Services Provider

Risk to Business: 1.201 = Extreme

Avem Health Partners has filed a data breach notification with the Maine's attorney general's office. Avem disclosed that patient information stored on servers of one of its vendors was subject to unauthorized access in an external hacking incident in May. Avem says that the breach was at a third-party data center the vendor in question used, 365 Data Centers. Further complicating the situation, that data center is disputing Avem's version of events. An estimated 271,000 people had information exposed in this incident. Patient information that may have been impacted in this breach includes names, birthdates, Social Security numbers, driver's license numbers, health insurance information and diagnosis/treatment information.

How It Could Affect Your Business: Supply chain risk is a huge problem for businesses that will only keep growing in 2023.

Iowa Public Broadcasting Service
https://therecord.media/royal-ransomware-group-claims-it-attacked-iowa-pbs-station/

Exploit: Ransomware

Iowa Public Broadcasting Service: Television Station

Risk to Business: 1.821 = Severe

The Royal ransomware group has claimed responsibility for a successful ransomware attack on Iowa's Public Broadcasting Station (PBS). The incident occurred on November 20, 2022. Iowa PBS said in a statement that the attack did not disrupt its ability to serve its viewers, and that all broadcast, livestream and digital platforms are still operational. However, local news outlets reported that the station had been forced to cut its annual fundraising drive short due to the cyberattack. It also appears that information was snatched by the gang. The station said that it sent out data breach notifications but has not specified who received them or what information was stolen.

How It Could Affect Your Business: Media organizations have been experiencing an increased level of cyberattacks, especially ransomware.

Jakks Pacific
https://therecord.media/toy-maker-jakks-pacific-reports-cyberattack-after-multiple-ransomware-groups-post-stolen-data/

Exploit: Ransomware

Jakks Pacific: Toymaker

Risk to Business: 1.981 = Severe

California-based toy company Jakks Pacific has disclosed that it was the victim of a successful ransomware attack. The company said that its servers were encrypted on December 8, 2022. Oddly, two major ransomware groups have posted data purportedly stolen from Jakks Pacific on their sites, Hive and BlackCat. Hive posted information allegedly snatched from Jakks Pacific first on December 19, 2022. BlackCat followed them with a post on December 28, 2022. The gangs featured screenshots of the reportedly stolen information on their individual leak sites. Hive's spokesperson told reporters that both gangs had purchased access to the data from an initial access broker, and they'd agreed to split the demanded $5 million ransom. The Hive representative also said that Jakks Pacific did not negotiate with the extortionists or pay the demanded ransom.

How It Could Affect Your Business: The Manufacturing sector has experienced a plague of cyberattacks that are compounding supply chain woes