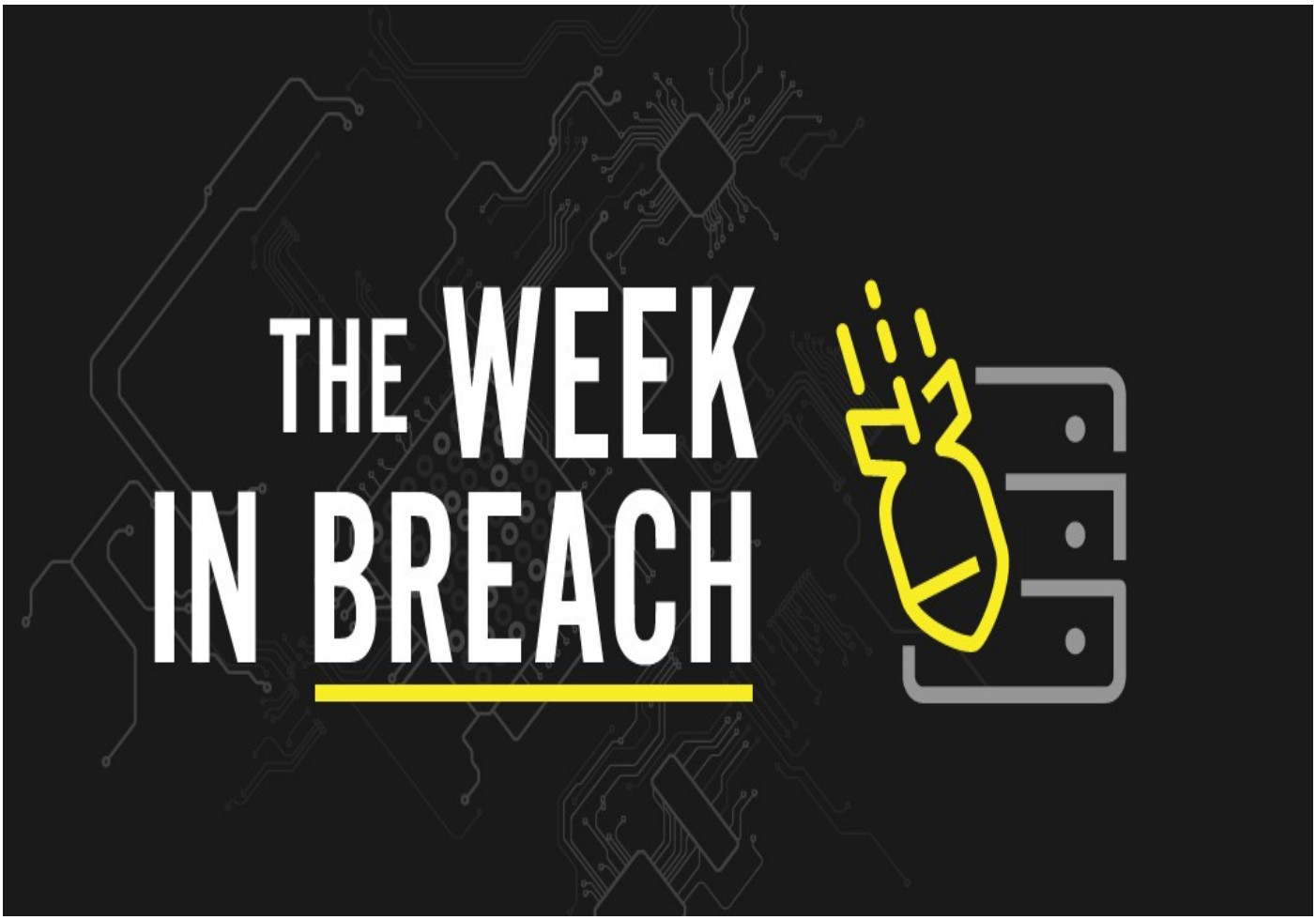
THE WEEK IN BREACH NEWS: 01/18/23 - 01/24/23

DenBe Computer Consulting
Connecting Business

January 25th. 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***

Bed, Bath and Beyond
https://www.reuters.com/business/retail-consumer/bed-bath-beyond-reviewing-possible-data-breach-2022-10-28/?utm_campaign=fullarticle&utm_medium=referral&utm_source=inshorts

Exploit: Phishing

Bed Bath and Beyond: Home Goods Retailer

Risk to Business: 2.776 = Moderate

The Vice Society ransomware gang has claimed responsibility for a cyberattack on the San Francisco Bay Area Rapid Transit (BART) system and added purportedly stolen data to its dark web leak site. NBC News reported that the gang snatched over 120,000 highly sensitive files from BART's police department that include data like the names of children suspected of suffering abuse, driver's license numbers and mental health evaluation forms. A spokesperson for BART says that no BART services or internal business systems have been impacted. No information was available at press time about any ransom demand.

How It Could Affect Your Business: Ransomware attacks have been an ongoing threat to infrastructure and the pace is not slowing down.

Consulate Health Care

https://securityaffairs.com/140452/cyber-crime/consulate-health-care-hive-ransomware.html

Exploit: Ransomware

Consulate Health Care: Healthcare Services Company

Risk to Business: 1.221 = Extreme

Consulate Health Care, a large provider of specialty healthcare services for seniors, has been hit by the Hive ransomware group. Hive recently leaked 550 GB of data that it claims to have stolen in the attack including PHI and PII. The attack took place on December 3rd, 2022, and it was disclosed on January 6, 2023. The gang claims to have stolen a wide array of data including contracts, NDA documents, proprietary company data (internally facing budgets, plans, evaluations, revenue cycle, investors relations, company structure, etc.), employee PII (social security numbers, emails, addresses, phone numbers, photos, insurances info, payments, etc.), and patient PII and PHI (medical records, credit cards, emails, social security numbers, phone numbers, insurances, etc.). This deluge of data was revealed on Hive's dark web leak site after Consulate Health Care apparently refused to pay an unspecified ransom.

How It Could Affect Your Customers' Business: This incident will cost Consulate a fortune once regulators get through with them.

Des Moines Public Schools
https://therecord.media/iowa-school-district-cancels-classes-another-day-due-to-cyberattack/

Exploit: Ransomware

Des Moines Public Schools: Municipal Education Authority

Risk to Business: 1.837 = Severe
Des Moines Public Schools, a system that serves more than 30k students, was forced to suspend classes for two days following a suspected ransomware on January 9. A district official said that the district was forced to take its systems offline after discovering the incident to limit the damage. The district was able to return to in-person learning on January 12. However, it experienced ongoing problems with its virtual learning and student information system Infinite Campus and its phone systems that have since been resolved. Many students were also left without Wi-Fi on campus, and access to networked systems within individual schools was also impacted.

How It Could Affect Your Customers' Business: The education sector is especially attractive to bad actors because of its time-sensitive nature.

Bay Bridge Administrators
https://www.securityweek.com/251k-impacted-data-breach-insurance-firm-bay-bridge-administrators

Exploit: Hacking

Bay Bridge Administrators: Employee Benefits Administrator

Risk to Business: 1.981 = Extreme

Texas-based employee benefits administration firm Bay Bridge Administrators says that it was the victim of a successful cyberattack that may have exposed the data of more than 250K people. Bay Bridge Administrators disclosed that on August 15, 2022, a threat actor gained unauthorized access to the Bay Bridge Administrators network and used that access to exfiltrate certain data on September 3, 2022. An investigation determined that PHI and PII was exposed in the incident, and subsequently began notifying those whose data had been stolen. The information about employees whose benefits Bay Bridge Administrators managed includes names, addresses, birth dates, Social Security numbers, ID and driver's license numbers and medical/health insurance data.

How It Could Affect Your Customers' Business: Business services companies like this one hold lots of valuable data, making them attractive targets for cyberattacks.