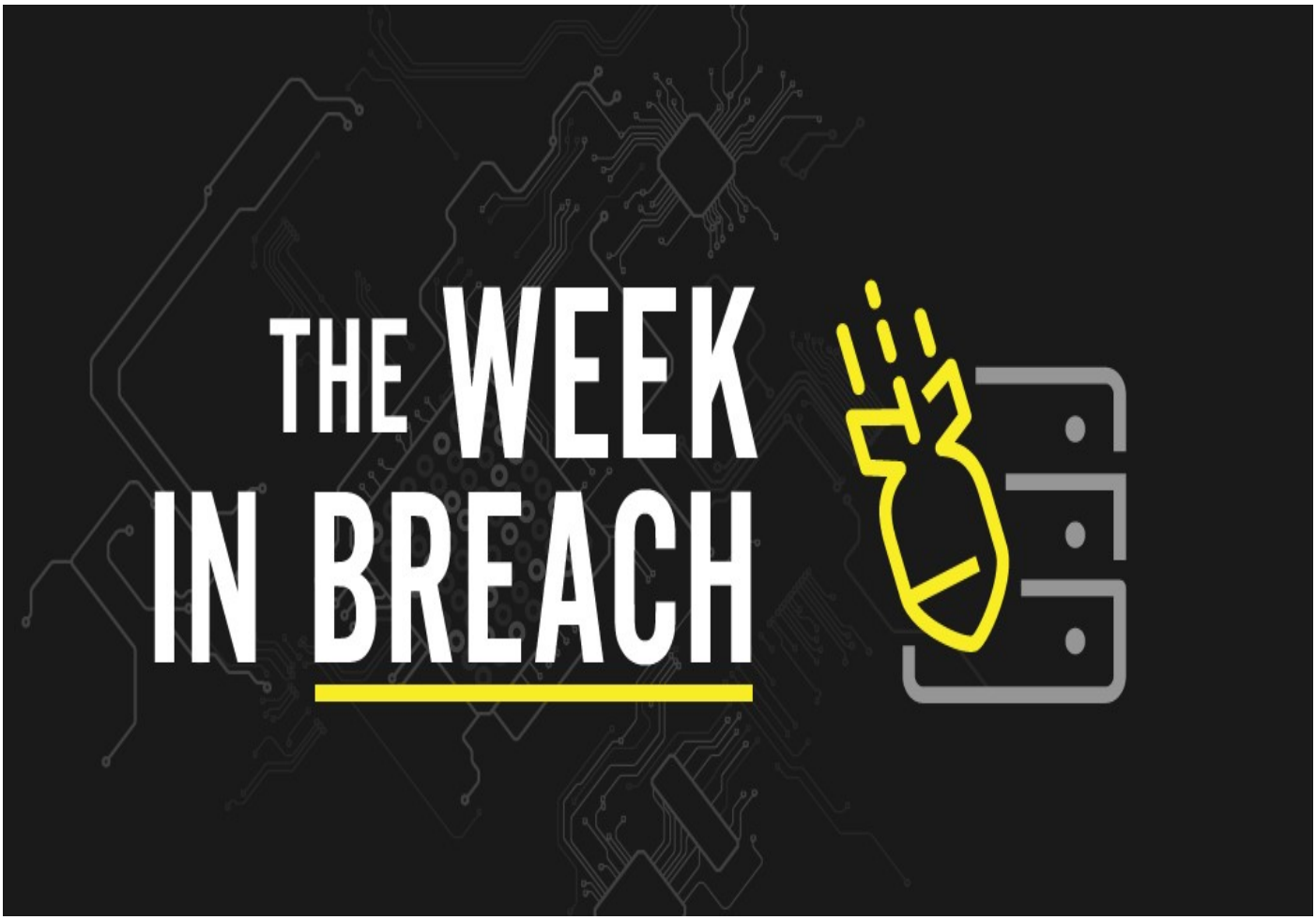
THE WEEK IN BREACH NEWS: 02/01/23 - 02/07/23

DenBe Computer Consulting
Connecting Business

February 7th 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***

One Brooklyn Health

https://www.scmagazine.com/analysis/breach/breach-notice-confirms-one-brooklyn-health-cyberattack-outage-in-november

Exploit: Hacking

One Brooklyn Health: Healthcare Provider

Risk to Business: 1.776 = Moderate

Hospital operator One Brooklyn Health has confirmed that its hospitals were forced offline in November 2022 because of a security incident. The incident affected three OBH hospitals and affiliated care sites: Brookdale Hospital Medical Center, Interfaith Medical Center and Kingsbrook Jewish Medical Center. At those hospitals, workers were forced to resort to manual recordkeeping, creating treatment delays that were widely reported in the local press. Bad actors gained access to patient data in the incident including patient names, dates of birth, billing and claims data, treatment details, medical record numbers, prescriptions and health insurance information.

How It Could Affect Your Business: Hospitals and medical facilities have been popular targets for bad actors and need extra security.

Zacks Investment Research
https://securityaffairs.com/141343/data-breach/zacks-investment-research-data-breach.html

Exploit: Hacking

Zacks Investment Research: Financial Analysts

Risk to Business: 2.021 = Severe

Investment analysis company Zacks Investment Research has informed more than 280,000 customers that bad actors gained access to some of its client data. The company said that the intrusion occurred at the end of 2022. In the incident, the intruders had their hands on a database of customers who had signed up for the Zacks Elite product between November 1999 and February 2005. Exposed data may include a customer's name, address, phone number, email address and password used for Zacks.com. Zacks was quick to assure customers that threat actors did not gain access to any customer credit card information, customer financial information or any other customer personal information.

How It Could Affect Your Customers' Business: The financial services industry was among the three most cyberattacked industries in 2022.

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

The municipal court system in Circleville, Ohio is the latest municipal government entity to have ransomware trouble. Circleville Municipal Court was added to the dark web leak site of the LockBit ransomware group last week. The group claims to have snatched 500 GB of data including sensitive court records. Officials have confirmed that the court system has had its operations disrupted and said that they are working with experts to get up and running again. No information was available about any ransom demands.

How It Could Affect Your Customers' Business: Ransomware has been a menace for government agencies and municipalities of all sizes.

GoTo

https://thehackernews.com/2023/01/lastpass-parent-company-goto-suffers.html

Exploit: Hacking

GoTo: Software Company

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: An incident like this could cost a company a fortune and not just in incident response – reputation damage is a consequence of a successful cyberattack.

Charter Communications

https://therecord.media/telecom-giant-charter-communications-says-third-party-vendor-had-security-breach/

Exploit: Supply Chain Attack

Charter Communications: Telecommunications Company

Risk to Business: 1.973 = Severe

Telecom giant Charter Communications disclosed that 550,000 of its customers have had information exposed as the result of a data breach at one of its vendors after bad actors claimed on a dark web site to have obtained Charter's customer data. A post on a dark web data broker's site claimed that the broker had obtained a tranche of data that belonged to Charter Communications that included 550K user records listing information like customers' account numbers and some identity information. Charter says that the incident is still under investigation. The company serves 32 million customers in 41 states.

How It Could Affect Your Customers' Business: Cybersecurity flubs by service providers can cause a cascade of supply chain problems that impact other businesses too.