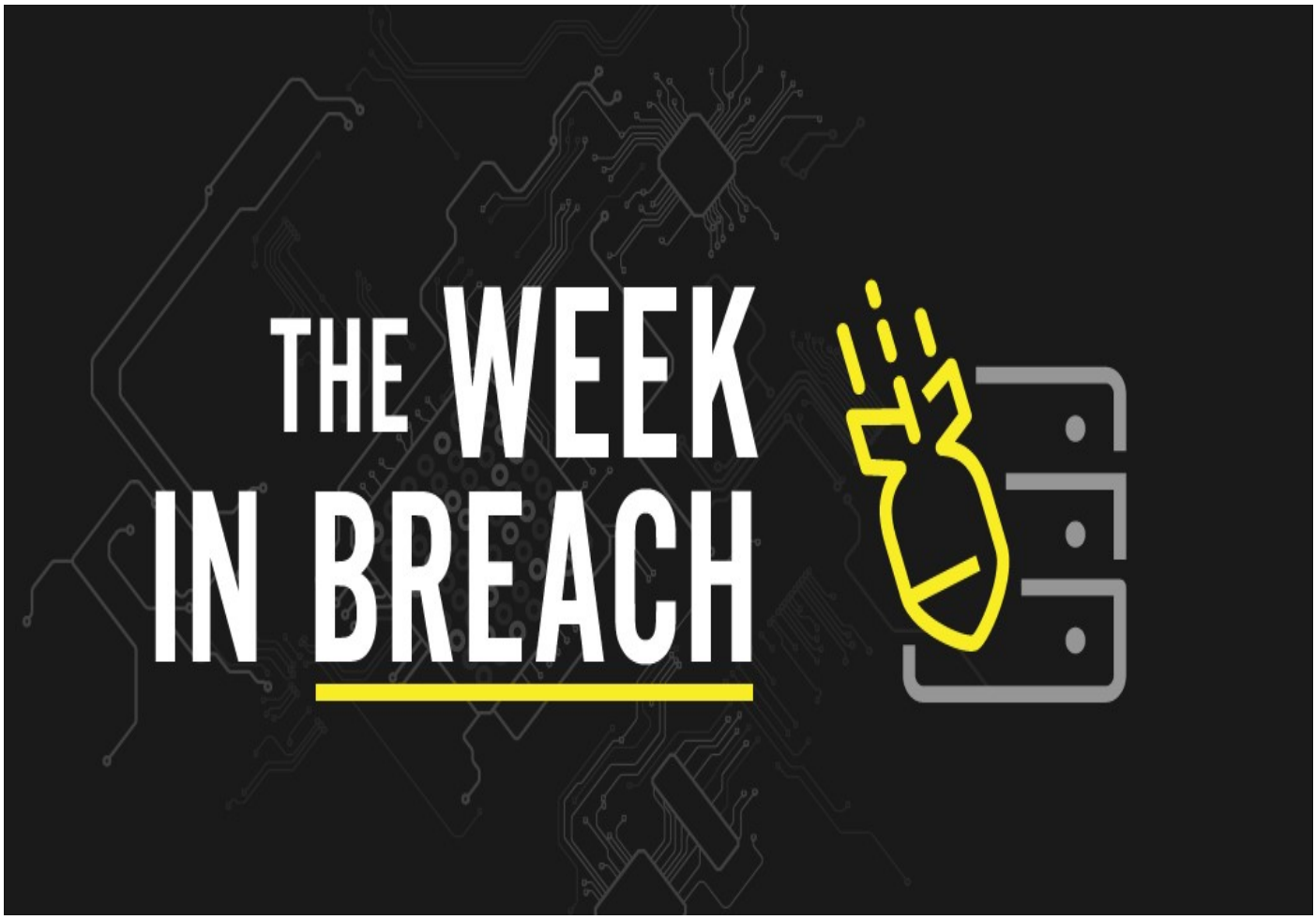
The Week in Breach News: 02/09/22 – 02/15/22

DenBe Computer Consulting
Connecting Business

February 16, 2022 by Dennis Jock



This week, hackers come calling at two telecoms, QR codes go wrong in Australia, an NFL team is defeated by ransomware and three unexpected approaches to overcome client and prospect objections and sell more security awareness training.

San Francisco 49ers

https://abcnews.go.com/Sports/wireStory/ransomware-gang-hacked-49ers-football-team-82865844

Exploit: Ransomware

San Francisco 49ers.: NFL Team

Risk to Business: 1.727=Severe

While everyone was focused on the big game last week, cybercriminals were focused on the San Francisco 49ers. The team was hit by a ransomware attack, purportedly by BlackByte. The cybercriminals claim they stole some of the football team's financial data, invoices and other internal documents. The team stressed the fact that this event appeared to be limited to their corporate network and did not endanger any fan or stadium databases.

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

Customers Impacted: Unknown

How It Could Affect Your Business *This is not an uncommon mistake, but it's always a problem and could be an expensive regulatory disaster in some industries*

EasyVote Solutions

https://www.govtech.com/security/georgia-voter-info-posted-online-after-software-company-breach

Exploit: Misconfiguration

EasyVote Solutions.: Voting Software Company

Risk to Business: 1.561=Severe

EasyVote Solutions has exposed some voter and poll worker data. The data was left unguarded and easily accessible on the internet. The software company says that exposed information does not include full voting records or registrations. The breach was discovered by South Carolina Law Enforcement Division (SLED) internet researchers. SLED and the FBI are investigating.

Individual Risk: 1.772=Severe

Exposed data for voters can include names, addresses, races and dates of birth. Exposed data for poll workers may include those details plus identity documents, Social Security numbers and financial data.

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

Customers Impacted: *3,000 so far*

How It Could Affect Your Business *Misconfiguration and sloppy security aren't uncommon mistakes, but they're always a problem and could be an expensive regulatory disaster in some industries.*

Meter

https://www.zdnet.com/article/4-4-million-stolen-in-attack-on-blockchain-infrastructure-meter/

Exploit: Hacking

Meter: De Fi Platform

Risk to Business: 1.279= Extreme

Another day, another DeFi hack. This time the victim was blockchain infrastructure company Meter. $4.4 million was stolen during a cyberattack on the Meter Passport platform in the form of 1391 ETH and 2.74 BTC. The incident also impacted Meter's Moonriver Network. The company acknowledged the hack on Saturday, urging users not to trade unbacked meterBNB circulating on Moonriver. The company says that it plans to repay some investors and the incident is under investigation. and it was taken in 3 separate transactions.

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

Customers Impacted: Unknown

How It Could Affect Your Business *De Fi continues to be a hotbed of hacking activity as cybercriminals seek quick scores of cryptocurrency, and there's still no end to the danger in sight.*

Memorial Hermann Health System

https://www.khou.com/article/news/local/memorial-hermann-cyberattack-security-breach/285-1cc8295d-48a4-452e-a6f2-1b4fd059f201

Exploit: Third-Party Breach

Memorial Hermann Health System: Healthcare Provider

Risk to Business: 1.861 = Severe

Memorial Hermann Health System is notifying patients that their data has been exposed after a data security incident at one of their service providers, Advent Health Partners. That company has been investigating unauthorized activity on company email accounts related to Memorial Hermann data. The incident was first spotted in September 2021.

Individual Risk 1.712 = Severe

An unauthorized third party accessed multiple files containing Memorial Hermann patients' protected health information (PHI) that may include first names, last names, dates of birth, social security numbers, driver's license numbers, financial information, health insurance information and treatment information.

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

Customers Impacted: 6,260

How it Could Affect Your Customers' Business *Organizations should keep in mind the fact that the preferred weapon of nation-state cybercriminals is ransomware.*