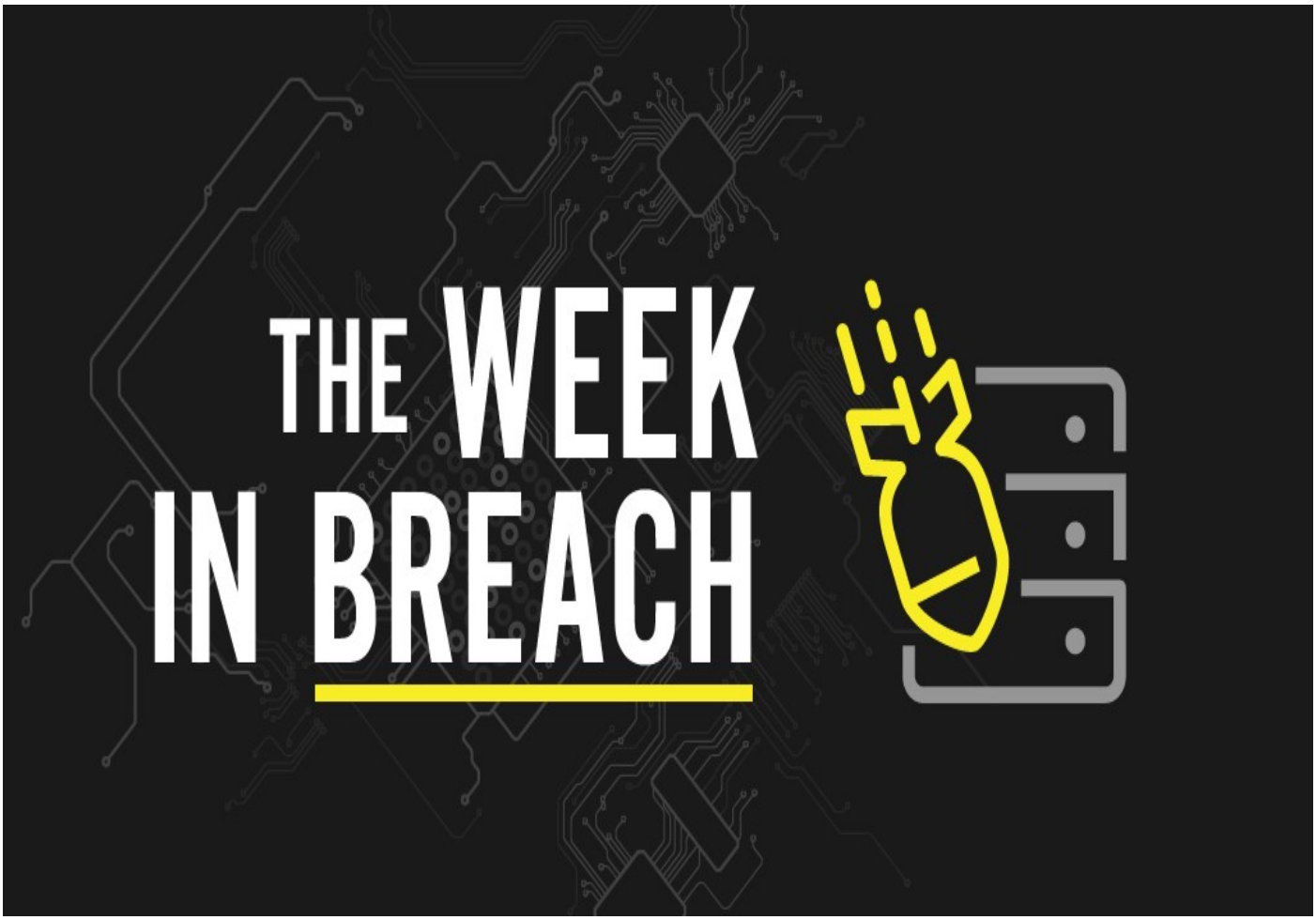
THE WEEK IN BREACH NEWS: 06/01/22—06/07/22

DenBe Computer Consulting
Connecting Business

August 11, 2022 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***

Aetna
https://www.bankinfosecurity.com/aetna-reports-326000-affected-by-mailing-vendor-hack-a-19691

Exploit: Supply Chain

Aetna: Insurer

Risk to Business: 2.631 = Moderate

Health insurance heavyweight Aetna has reported a data breach to federal regulators affecting nearly 326,000 individuals. This breach was spurred by a ransomware attack at a service provider for an Aetna subcontractor, mailing company OneTouchPoint. This incident is one of the first reported as a direct result of that cyberattack. The OneTouchPoint breach is expected to impact over 30 large and small health insurers and plan providers.

Individual Risk: 2.755 = Moderate

Aetna said that the exposed information for individuals may include names, addresses, dates of birth, and limited medical information.

How it Could Affect Your Business: Business services companies are becoming choice targets for cybercriminals looking for quick scores of data.

Lin-Mar School District
https://www.kcrg.com/2022/08/03/leaked-image-shows-ransomware-attack-hit-linn-mar-school-district/

Exploit: Ransomware

Risk to Business: 2.372 = Severe

Thanks to a bit of timely reporting by local media, it has been revealed that the Lin-Mar School District in Iowa has become a victim of the Vice Society ransomware group. Screenshots of the group's ransom note were given to the media by an anonymous district staff member. This leak occurred after the school district informed parents and students that it was suffering unspecified "technical difficulties", raising concerns about the district's readiness to open for the new school year. The school district has so far refused further comment.

Individual Impact: No information about consumer/employee PII, PHI or financial data exposure was available at press time.

Wisan Smith Racker & Prescott
https://www.jdsupra.com/legalnews/wisan-smith-racker-prescott-confirms-5913417/

Exploit: Hacking

Wisan Smith Racker & Prescott: Accounting Firm

Risk to Business: 1.716 = Severe

Salt Lake City Utah Based accounting firm Wisan Smith Racker & Prescott has disclosed that they have experienced a data breach. On June 14, 2022, the firm learned that an unauthorized party had penetrated its IT security and accessed information about their clients. That information was subsequently used to file fraudulent tax returns supposedly on behalf of several of the company's clients. Data breach letters have been sent to all of the clients impacted by this breach.

Individual Risk: 1.788 = Severe

The exposed information varies depending on the individual, but it may include a clients' name, Social Security number, driver's license or state identification card number, passport number, military identification number, government-issued identification number, financial account information, date of birth, electronic signature, medical information and health insurance information.

How it Could Affect Your Business: Ransomware attacks on service providers in the supply chain are an ongoing problem that won't be going away anytime soon.

Goodman Campbell Brain and Spine
https://www.bankinfosecurity.com/neuro-practice-tells-363000-that-phi-was-posted-on-dark-web-a-19706

Exploit: Ransomware

Goodman Campbell Brain and Spine: Specialty Medical Practice

Risk to Business: 1.719 = Severe

Goodman Campbell Brain and Spine, a medical practice in Indiana, has disclosed that it has experienced a data breach as a result of a suspected ransomware attack. The Hive ransomware group is implicated in the attack. The practice noted that they discovered the attack had been successful on May 20, 2022. An estimated 363,000 people had data exposed in this incident.

Individual Risk: 1.606 = Severe

Information affected in the incident includes patient PII and PHI including name, date of birth, address, telephone number, email addresses, medical record number, patient account number, diagnosis and treatment information, physician name, insurance information, dates of service and Social Security numbers.

How it Could Affect Your Business: Healthcare is the industry with the highest data breach cost, and its' been beleaguered by ransomware.

American Marriage Ministries (AMM)
https://therecord.media/american-marriage-ministries-acknowledges-data-exposure-after-earlier-incident-reported-to-fbi/

Exploit: Misconfiguration

American Marriage Ministries (AMM): Non-Profit

Risk to Business: **2.617 = Moderate**

American Marriage Ministries (AMM), a Seattle-based non-denominational religious organization that ordains wedding officiants, has suffered a data breach. Researchers say they've discovered 630 GB of data on about 185,000 officiants and roughly 15,000 married couples as well as their wedding guests exposed in an unsecured Amazon Web Services bucket. The data trove contained Ministers' program application forms, over 500,000 ordination certificates and minister identification documents, and marriage licenses that contain details about newly wedded couples and more was included in the bucket. The incident was reported to FBI IC3.

Individual Impact: No information about consumer/employee PII, PHI or financial data exposure was available at press time.

How it Could Affect Your Business: SMBs that handle or store large amounts of data have been high on cybercriminal shopping lists, particularly in recent months.