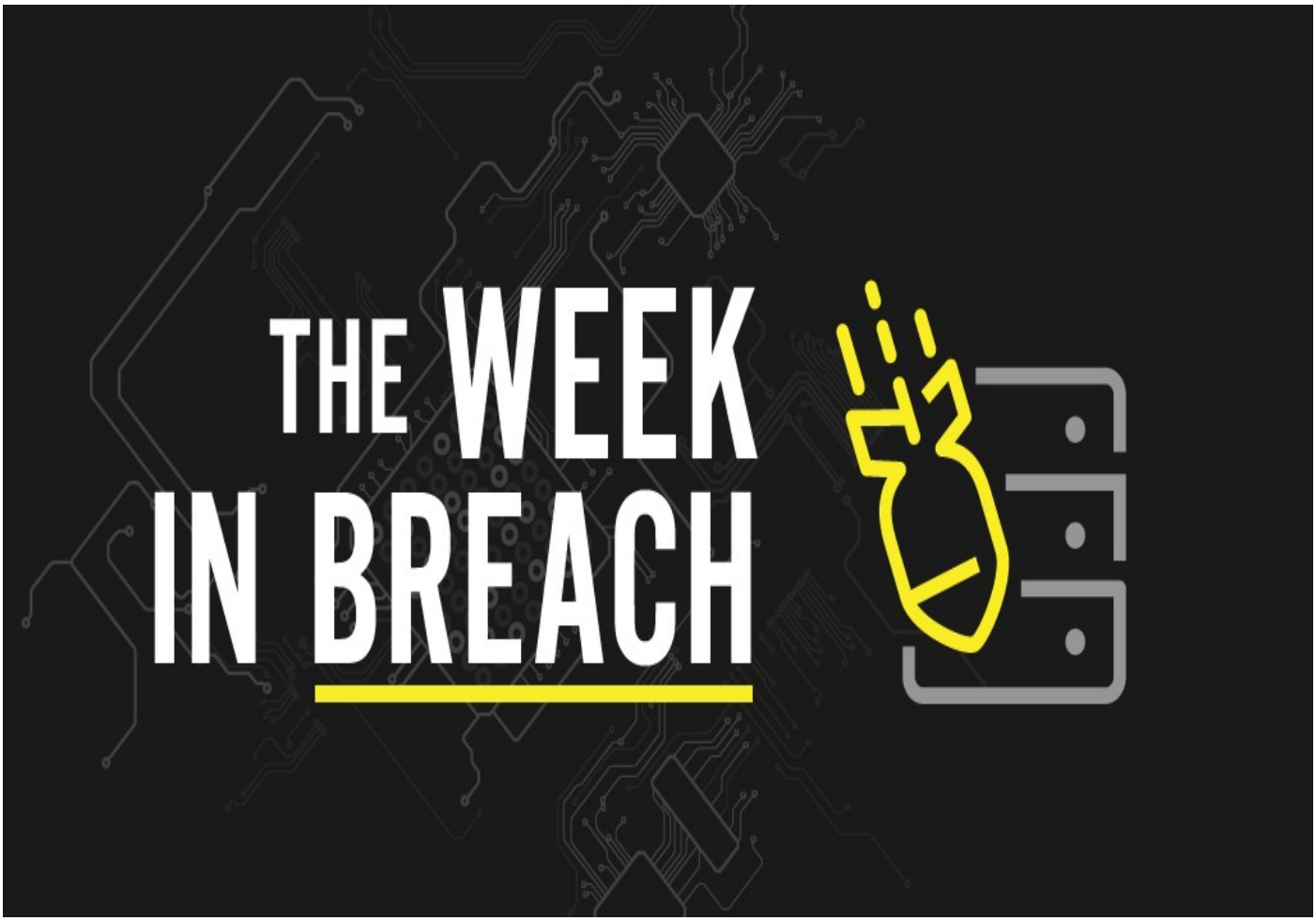
THE WEEK IN BREACH NEWS: 06/01/22—06/07/22

DenBe Computer Consulting
Connecting Business

July 14, 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***

Marriott International
https://www.cyberscoop.com/marriott-data-breach-baltimore/

Exploit: Ransomware

Marriott International: Hotel Operator

Risk to Business: 2.783 = Moderate

Marriott is looking at another big data breach after a group of cybercriminals claims to have stolen an estimated 20 gigabytes of data, including financial data like credit card information and confidential information about guests and workers from an employee at the BWI Airport Marriott in Baltimore. The group identified themselves as GNN or "Group with No Name" to media outlets and sent along samples of the purportedly stolen data. Marriott contends that the stolen data consisted of "non-sensitive internal business files regarding the operation of the property." The incident remains under investigation.

How It Could Affect Your Business: Hotels are a prime target for cybercriminals because they often have stores of valuable financial and personal data on guests.

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.

SHI International
https://www.bleepingcomputer.com/news/security/it-services-giant-shi-hit-by-professional-malware-attack/

Exploit: Malware

SHI International: IT Services

Risk to Business: 1.601 = Severe

New Jersey-based IT services provider SHI international suffered a major business disruption over the July 4 weekend after being forced offline by a cyberattack. The company disclosed that the defensive measures it had been forced to take to stop the attack included taking SHI's public websites and email offline while the attack was investigated. Website and email outages lasted for several days before finally being resolved about July 10. Customers were told that they could still access their representatives by phone throughout the incident which remains under investigation.

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

How it Could Affect Your Business: MSPs, MSSPs and other IT/technical services providers have been frequent targets of cybercriminals recently and should strengthen security.

Risk to Business: 1.903 = Severe

A ransomware attack that landed on Yuma Regional Medical Center (YRMC) in Arizona has exposed the protected health information of an estimated 700,000 patients. The company has disclosed that it experienced the ransomware attack in late April and that an unauthorized individual had access to YRMC's systems from April 21 to April 25, allowing them to steal a subset of files from the systems. There was no impact on patient care.

Risk to Business: 1.903 = Severe

A ransomware attack that landed on Yuma Regional Medical Center (YRMC) in Arizona has exposed the protected health information of an estimated 700,000 patients. The company has disclosed that it experienced the ransomware attack in late April and that an unauthorized individual had access to YRMC's systems from April 21 to April 25, allowing them to steal a subset of files from the systems. There was no impact on patient care.

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

How it Could Affect Your Business: A data breach for a healthcare organization is especially damaging between incident costs and regulatory penalties.

WellDyneRx, LLC
https://www.jdsupra.com/legalnews/welldynerx-llc-files-notice-of-data-1085442/

Exploit: Hacking

WellDyneRx, LLC: Pharmacy Benefits Management

Risk to Business: 2.304 = Severe

WellDyneRx has reported a data breach that resulted from unauthorized access to one of the company's email accounts. The company filed a notice with the U.S. Department of Health and Human Services Office for Civil Rights regarding a data breach in December 2021, indicating that the company estimates the breach affected 38,401 individuals. WellDyneRX is a pharmacy benefit manager and oversees the administration of the pharmacy benefits portion of insurance policies on behalf of insurance companies at 65,000 retail pharmacies from major chains to mom-and-pop shops.

Individual Risk: 2.215 = Severe

Cybercriminals may have accessed the names, dates of birth, Social Security numbers, driver's license numbers, treatment information, health insurance information, contact information, prescription information, and other medical and healthcare-related information of individuals served by WellDyneRx.

How it Could Affect Your Business: It's not just hospitals and doctor's offices, medical services providers are also experiencing surging risk with big penalties for failure to keep data safe.