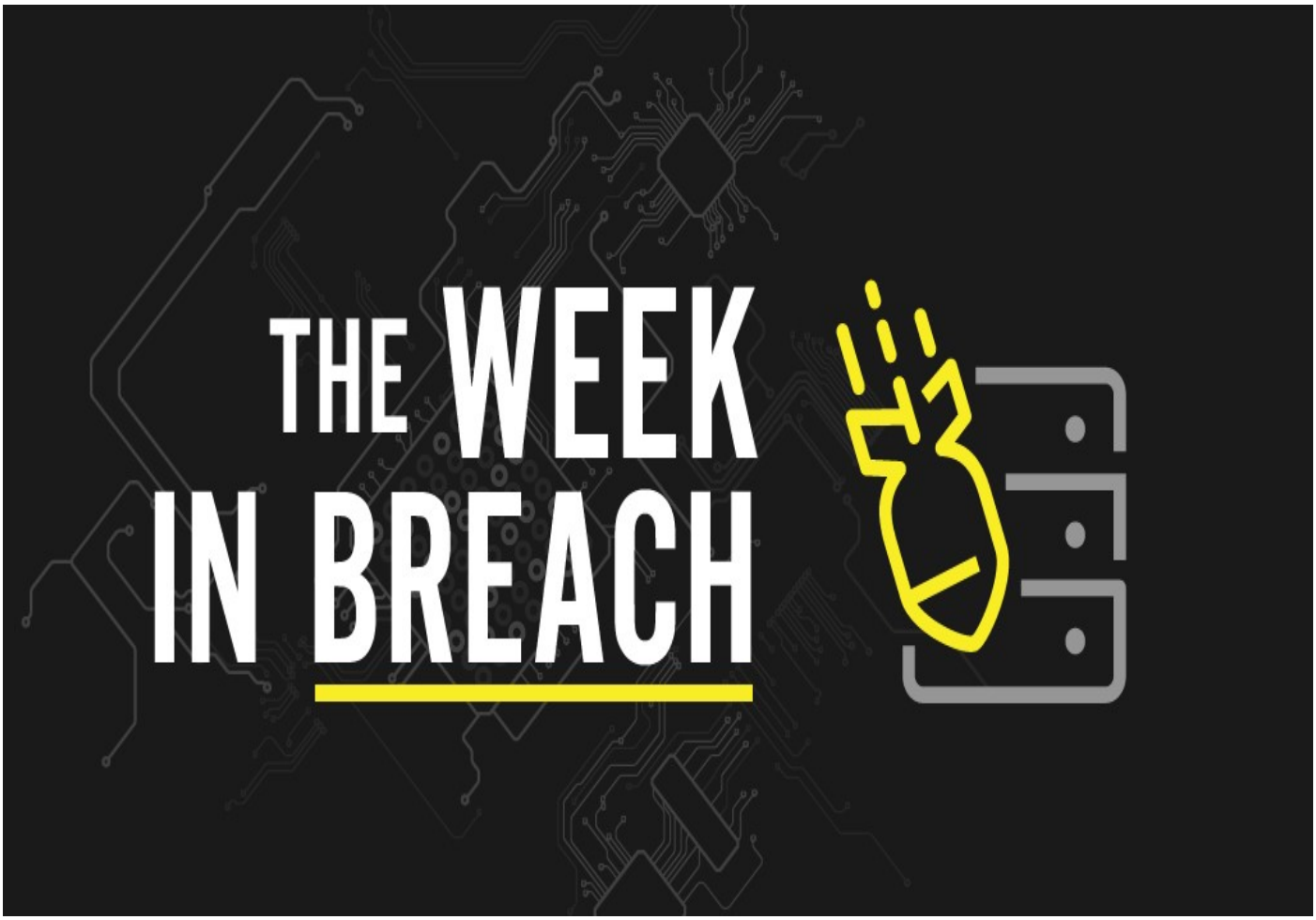
THE WEEK IN BREACH NEWS: 08/10/22 – 08/16/22

DenBe Computer Consulting
Connecting Business

August 24th, 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***

Cisco
https://www.theregister.com/2022/08/11/cisco_corporate_network_compromised/

Exploit: Hacking

Cisco: Networking Technology Company

Risk to Business: 1.672 = Severe

Kansas-based managed service provider NetStandard suffered a cyberattack that resulted in the company pressing pause on its MyAppsAnywhere cloud services, consisting of hosted Dynamics GP, Exchange, Sharepoint and CRM services. The MSP detected signs of a cyberattack last Tuesday morning and quickly shut down cloud services to prevent the attack's spread. The company announced that only the MyAppsAnywhere services are affected, but news outlets report that the attack may have had a broader impact, with the company's main site shut down as well.

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

How It Could Affect Your Business: Insecure or compromised employee credentials can do big damage in a very short span of time.

PlatformQ
https://vpnoverview.com/research/platformq-exposes-personal-info-of-nearly-100000-us-healthcare-workers/

Exploit: Misconfiguration

PlatformQ: Digital Engagement Solutions

Risk to Business: 1.687 = Severe

PlatformQ, a provider of digital engagement solutions for healthcare (PlatformQ Health) and education (PlatformQ Education) sector entities, experienced a data breach after an employee accidentally published a database backup stored in a misconfigured AWS S3 bucket. The data appears to be about marketing the drug Zarex to doctor's offices and similar places, and PII for healthcare professionals was involved.

Individual Risk: 1.733 = Severe

The leak exposed sensitive information including the full names, personal email addresses, job titles work email addresses, home, work and private phone numbers and National Provider Identifier (NPI) numbers of an estimated 99,000 healthcare professionals

How it Could Affect Your Business: Employee mistakes and negligence are responsible for more data breaches than any other cause, but training helps fix that.

Behavioral Health Group

https://www.scmagazine.com/analysis/breach/behavioral-health-group-informs-198k-patients-of-data-theft-from-december

Exploit: Hacking

Behavioral Health Group: Addiction Treatment Center Operator

Risk to Business: 1.716 = Severe

Behavioral Health Group recently began notifying 197,507 patients that their data was stolen in a December 2021 cyberattack. The opioid treatment provider's 80 clinics suffered a week of IT outages that disrupted patient care after a cyberattack forced the team to shut down portions of the network. That in turn caused delays for health services like refilling patient medications, a critical part of the recovery process for many addiction treatment patients.

Individual Risk: 1.802 = Severe

The stolen data varied by patient and could include patient names, Social Security numbers, driver's licenses, passports, biometrics, health insurance information, diagnoses, treatments, prescriptions, dates of service, and medical record numbers. Only patients whose SSNs were compromised will receive free credit monitoring.

How it Could Affect Your Business: Medical entities of all sorts have been high on cybercriminal hit lists because they know that it's a rich and time-sensitive industry.

Acorn Financial Services
https://www.jdsupra.com/legalnews/acorn-financial-services-reports-data-5996771/

Exploit: Phishing

Acorn Financial Services: Financial Planners

Risk to Business: 1.837 = Severe

In April 2022, Acorn Financial Services discovered unusual activity within an employee email account that ultimately led to uncovering a data breach. Acorn says that the incident was kicked off by an employee falling for a phishing email. The company acted to secure the employee's email account and confirmed that an unauthorized actor has potentially gained access to sensitive customer data. The company has filed data breach notifications and is informing the impacted customers via mail.

ndividual Risk: 1.646 = Severe

While the breached information varies depending on the individual, it may include the client's name, address, date of birth, driver's license number, financial account number, Social Security number and other account-related information.

How it Could Affect Your Business: The financial services sector was the most heavily under seige by ransomware last year, a pattern that continues in 2022.

Klaviyo
https://www.bleepingcomputer.com/news/security/email-marketing-firm-hacked-to-steal-crypto-focused-mailing-lists/

Exploit: Phishing

Klaviyo: Email Marketing Firm

Risk to Business: 2.284 = Severe

In an interesting twist on the usual data breach incident, email marketing firm Klaviyo suffered a concentrated and specific data breach on August 3, 2022. After gaining access to an employee's account thanks to a successful phishing attack, bad actors then downloaded marketing lists used by cryptocurrency-related clients for outreach efforts and for Klaviyo product and marketing updates. The threat actor used the internal customer support tools to search for primarily crypto-related accounts and viewed list and segment information for 44 Klaviyo accounts, downloading data from at least 38 accounts.

Risk to Business: 2.284 = Severe

Stolen data includes customers' names, addresses, email addresses, account profile information and phone numbers. The hackers also downloaded two internal lists used by Klaviyo for product and marketing updates that contain names, addresses, email addresses, and phone numbers.

How it Could Affect Your Business: Phishing is the most likely way for any organization to open the door to a data breach.