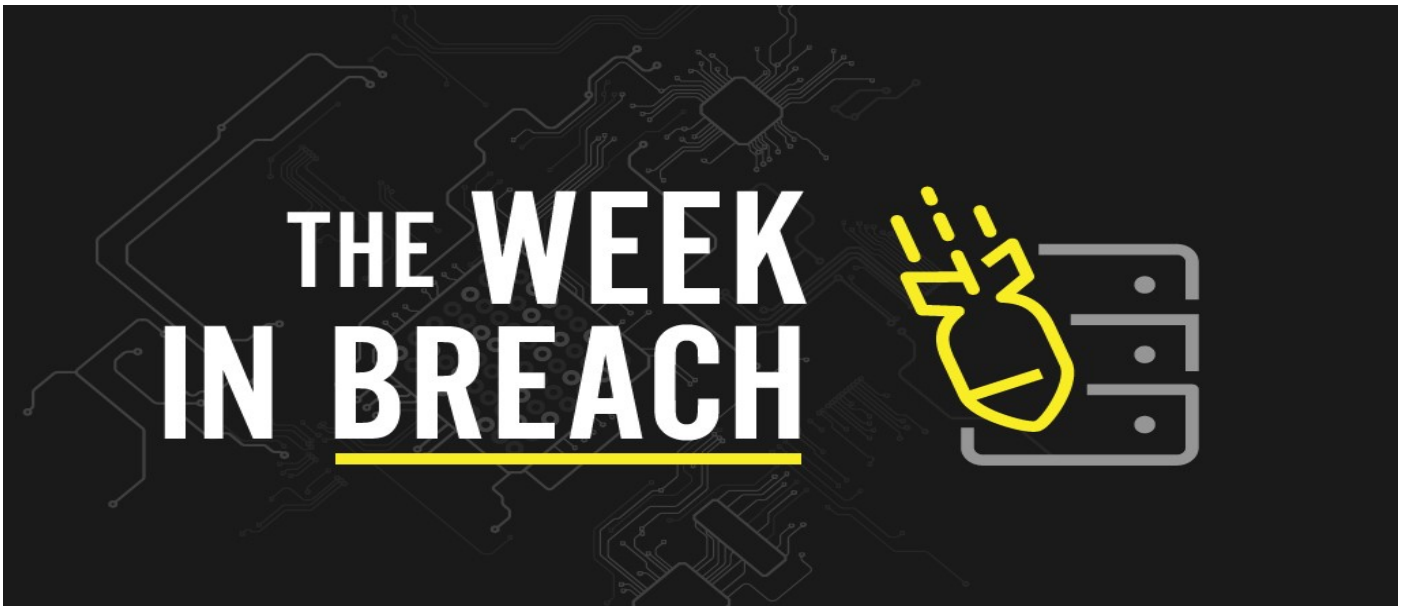
THE WEEK IN BREACH NEWS: 03/10/21 – 03/16/21

DenBe Computer Consulting
Connecting Business

March 17, 2021 by Dennis Jock

This Week in Breach News:

Molson Coors goes dry after a cyberattack impacts production.



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***

Molson Coors

https://edition.cnn.com/2021/03/11/tech/molson-coors-cybersecurity-hack/index.html

Exploit: Hacking

Molson Coors: Brewing Conglomerate

Risk to Business: 1.727 = Severe

Molson Coors told regulators that they've experienced a serious cybersecurity incident. The hack has taken its systems offline, delaying and disrupting parts of Molson Coors' operations, including its production and shipments.

Individual Impact: No sensitive personal or financial information was announced as part of this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Hacking that disrupts production is a big problem, and reassessing cybersecurity training is a good idea after a serious incident like this.

Premier Diagnostics

https://www.infosecurity-magazine.com/news/utah-company-unsecured-server/

Exploit: Unsecured Database

Premier Diagnostics: Medical Testing

Risk to Business: 1.872 = Severe

Utah medical testing company Premier Diagnostics has exposed the sensitive information of more than 50,000 customers by storing personally-identifying information on an unsecured server. The breach at Premier Diagnostics was discovered by researchers and contains sensitive customer data including scans of passports, health insurance ID cards, and driver's licenses. Patients affected are from Utah, Nevada and Colorado.

Individual Risk: 1.612 = Severe

Patients should be aware of this information being used for identity theft and spear phishing.

Customers Impacted: 50,000

How it Could Affect Your Business: Sensitive PII requires strong protection, especially in the medical sector, because failure to keep it safe incurs huge fines. .

University of Texas at El Paso

https://www.infosecurity-magazine.com/news/hackers-target-texas-university/

Exploit: Hacking

University of Texas at El Paso: Institution of Higher Learning

Risk to Business: 2.212 = Severe

The computer network of the University of Texas at El Paso had to be shut down as technicians discovered a significant cyberattack in progress. Email and the server hosting the university's website were affected by the incident, forcing faculty and students to communicate via Blackboard. The cyber-attack has also led to the closure of the university's walk-up COVID-19 testing sites.

Individual Impact: No sensitive personal or financial information was announced as part of this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Hackers can disrupt large parts of an operation fast, leaving businesses scrambling to get back to work and causing lost revenue.

Cochise Eye & Laser

https://www.infosecurity-magazine.com/news/ransomware-attack-on-arizona/

Exploit: Ransomware

Cochise Eye and Laser: Optometry

Risk to Business: 1.727 = Severe

A ransomware incident at an optometrist located in Sierra Vista, Arizona, has affected up to 100,000 patients. In a recent breach notice, Cochise Eye and Laser informed regulators that the practice has been hit by ransomware, encrypting the office's patient scheduling and billing software.

Individual Risk: 1.603 = Severe

Patient data stored in the billing software included names, dates of birth, addresses, phone numbers, and in some cases Social Security numbers. There is no evidence that data was exfiltrated, but customers of this practice should be ready for potential identity theft or phishing.

Customers Impacted: Unknown

How it Could Affect Your Business: This is a tremendous problem for businesses of every size, and even without confirmation that data was stolen the practice will be dinged with a substantial fine.