THE WEEK IN BREACH NEWS: 06/08/22-06/14/22

DenBe Computer Consulting
Connecting Business

June 16, 2022 by Dennis Jock

More trouble for two of 2021's most ransomware-prone sectors, a detailed map of exactly how ransomware hit a Japanese hospital and a look at the 6 major influences responsible for today's threat landscape and the threats of tomorrow.

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***

Tenafly Public Schools
https://www.govtech.com/education/k-12/new-jersey-district-cancels-finals-after-ransomware-attack

Exploit: Ransomware

Risk to Business: 2.827 = Moderate

Tenafly Public Schools was forced to cancel student final exams and resort to low-tech teaching methods to finish out the school year after ransomware had encrypted data on some computers in the district's network. A Tenafly Public School District spokesperson said that administrators first identified the security incident Thursday and discovered that it involved the encryption of data by ransomware on some computers in the district's network.

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

How It Could Affect Your Business: Schools and education sector organizations at every level have been prime targets for cybercrime in the last few years.

Private Client Services, LLC.
https://www.jdsupra.com/legalnews/compromised-email-account-leads-to-data-9566510/

Exploit: Hacking

Private Client Services LLC. : Financial Services

Risk to Business: 1.801 = Severe

Private Client Services, LLC ("PCS") has disclosed a data breach that the company is blaming on an unauthorized party gaining access to sensitive consumer information through a compromised employee email account. The company sent data breach letters to 22,554 impacted people on May 27, 2022.

Risk to Business: 1.822 = Severe

According to PCS, the breach resulted in the names, Social Security numbers, driver's license numbers and state identification numbers being compromised.

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

How it Could Affect Your Business :Financial Services & Banking was the sector that experience the most ransomware attacks in 2021 and that pace isn't slowing down.

Aesto Health
https://www.securityweek.com/ransomware-group-claims-have-breached-foxconn-factory

Exploit: Hacking

Aesto Health: Medical Information Services Provider

Risk to Business: 1.976 = Severe

Aesto Health has announced it recently experienced a cyberattack that caused disruption to certain internal IT systems. The Alabama-based company disclosed that it had experienced a security breach that was detected on March 8, 2022. Aesto Health has brought in a third-party computer forensics company to assist with the investigation. They've also determined that an unauthorized individual had access to the affected systems from December 25, 2021, to March 8, 2022.

Risk to Business: 1.915 = Severe

A review of the affected files confirmed they contained patients' protected health information, including names, dates of birth, physician names, and report findings related to radiology imaging at Osceola Medical Center (OMC) in Wisconsin. No Social Security numbers or financial information were viewed or stolen,

How it Could Affect Your Business : Healthcare providers in the US don't just have to worry about the standard expenses of a data breach, they face big regulatory penalties too

OnDeck Capital
https://www.jdsupra.com/legalnews/ondeck-announces-data-breach-impacting-8105356/

Exploit: Hacking

OnDeck Capital: Financial Services

Risk to Business: 1.976 = Severe

OnDeck has disclosed that the company experienced a data breach after an unauthorized party gained access to the company's computer network and transferred sensitive data to a private cloud storage account. OnDeck says that it first detected suspicious activity on March 10 and immediately shut down access to all affected devices. But three days later, OnDeck determined that the attackers had copied sensitive data to a private cloud storage account

Risk to Business: 1.721 = Severe

The customer data that was compromised may include names, Social Security numbers, tax ID numbers, driver's license numbers, passport numbers, financial account/payment card account numbers, and medical or health insurance information.

How it Could Affect Your Business : Entities in the financial services sector need to take extra precautions against trouble because it was 2021's hardest hit sector for ransomware attacks.