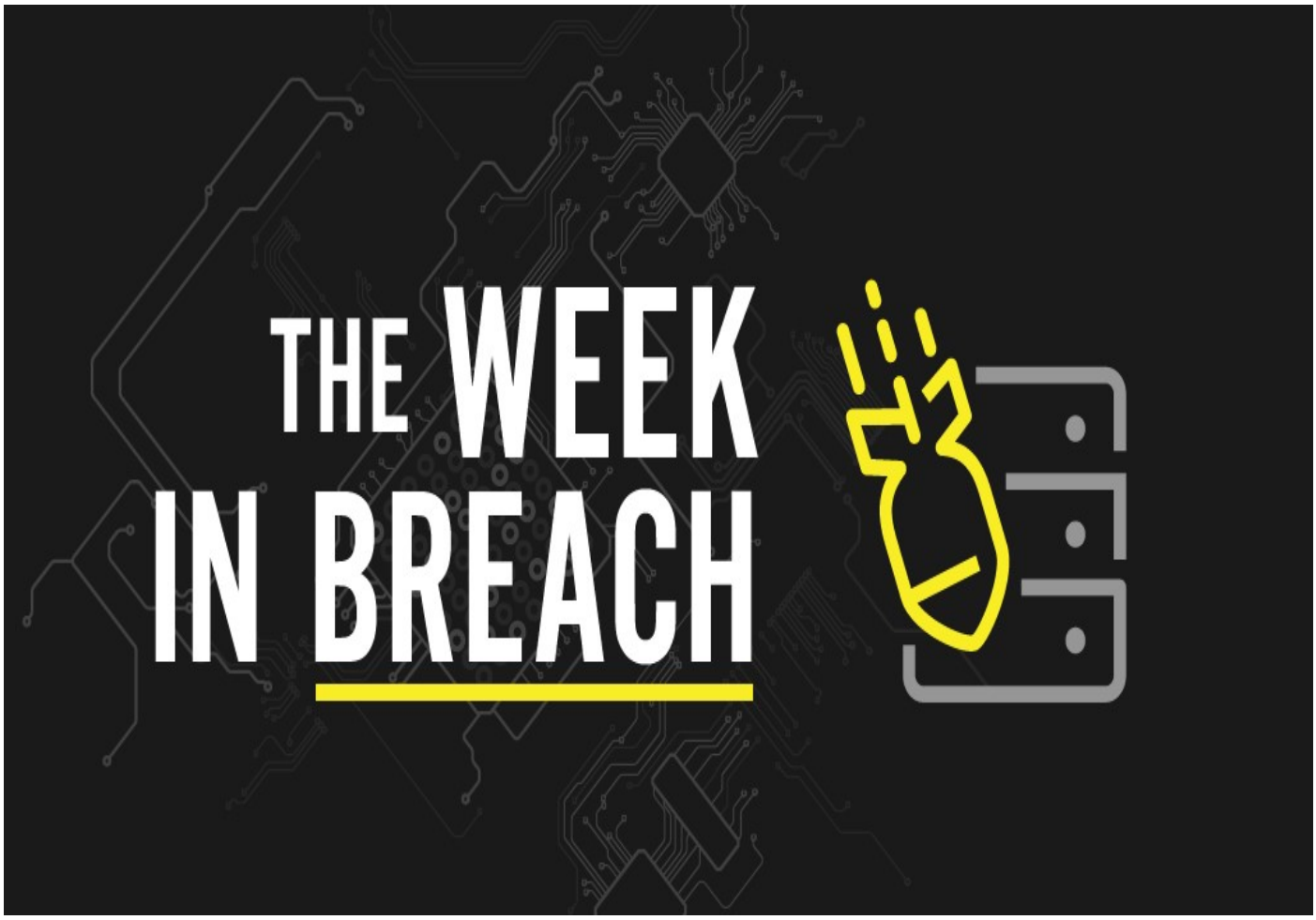
THE WEEK IN BREACH NEWS: 01/19/22 – 01/25/22

DenBe Computer Consulting
Connecting Business

January 26th, 2022 by Dennis Jock



A cyberattack impacting the International Red Cross endangers refugees, phishing costs a US city over $200K, more crypto and financial sector trouble and inside 2021's data breach landscape to see who got hit and how it happened.

RR Donnelly

https://www.bleepingcomputer.com/news/security/marketing-giant-rrd-confirms-data-theft-in-conti-ransomware-attack/

Exploit: Ransomware

RR Donnelly: Marketing & Communications Firm

Risk to Business: 1.227= Severe

Major marketing company RR Donnelly has disclosed that they had data stolen in a December cyberattack attributed to ransomware. The Conti ransomware group is suspected to be to blame. In the attack on December 27, 2021, the company experienced a systems intrusion that led it to shut down its network to prevent the attack's spread. That led to disruptions for customers, with some unable to receive printed documents required for vendor payments, disbursement checks and motor vehicle documentation. The Conti ransomware gang claimed responsibility on January 15 and began leaking 2.5GB of the stolen data that has since been removed.

Individual Impact: No specifics about consumer/employee PII or financial data loss were available at press time.

Customers Impacted: Unknown

How It Could Affect Your Business: *A recent rash of ransomware attacks against media and communications organizations should have everyone in that sector on notice.*

Strategic Benefits Advisors, Inc

https://www.jdsupra.com/legalnews/data-breach-alert-strategic-benefits-8267696/

Exploit: Hacking

Strategic Benefits Advisors: Human Resources Consulting Firm

Risk to Business: 2.223 =Severe

In a recent legal filing, Strategic Benefits Advisors disclosed that an unauthorized third party had gained access to its data and may have removed several files containing consumer information. The Georgia-based company provides full-service employee benefits consulting for companies in many industries.

Individual Risk: 2.419=Severe

Strategic Benefits Advisors sent breach notification letters to more than 58,000 people to inform them of the exposure which the company says was limited to full names and Social Security numbers.

Customers Impacted: Unknown

How It Could Affect Your Business *Hackers have been especially interested in breaching companies that maintain large stores of data for other companies lately.*

City of Tenino, Washington

https://www.govtech.com/security/washington-city-loses-280-309-to-successful-phishing-scam

Exploit: Phishing/BEC

City of Tenino, Washington: Municipality

Risk to Business: 1.717= Severe

The City of Tenino, Washington is down $280,309 in public funds according to the Washington State Auditor's Office after a city employee fell for a phishing message that launched a business email compromise scam. Reports say that former Clerk Treasurer John Millard fell victim to a phishing message and paid cybercriminals a boatload of money, some without city council approval. The official reportedly initiated 20 automated clearing house payments from the city's bank account to multiple out-of-state bank accounts. News outlets are also reporting that a warning was sent out to clerks about the phishing scam immediately but that didn't stop this disaster from happening.

Individual Impact: No specifics about any consumer/employee PII or financial data loss were available at press time.

Customers Impacted: Unknown

How It Could Affect Your Business *BEC is the most expensive cybercrime according to the FBI, 64X more expensive than ransomware – and it usually starts with phishing.*