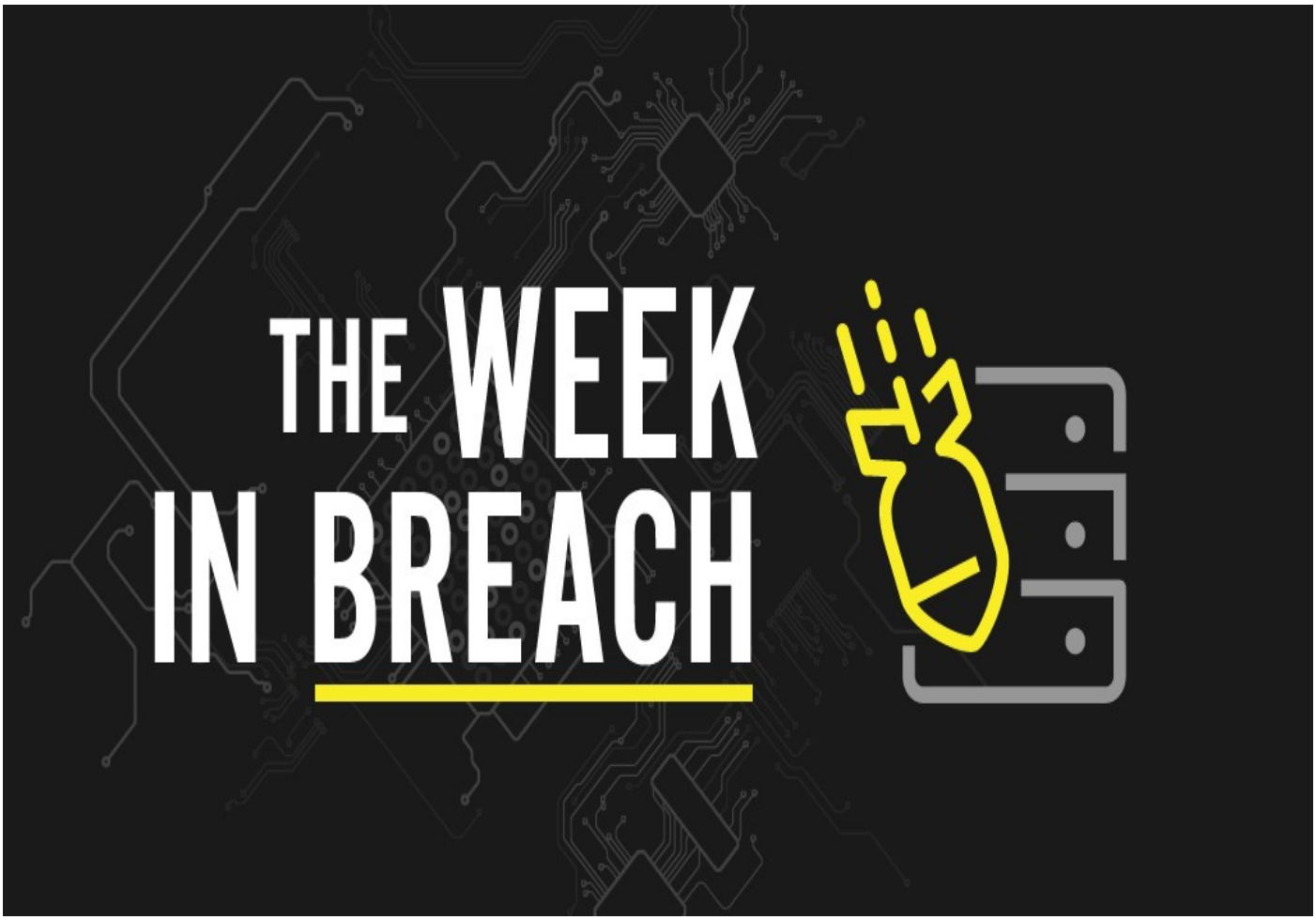
THE WEEK IN BREACH NEWS: 09/28/22 - 10/04/22

DenBe Computer Consulting
Connecting Business

October 5, 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***

The City of Wheat Ridge, CO
https://www.denverpost.com/2022/09/22/wheat-ridge-ransomware-fremont-county-cyber-attack/

Exploit: Ransomware

The City of Wheat Ridge, CO: Municipal Government

Risk to Business: 2.175 = Severe

A Colorado city is putting its IT systems back in order after a successful cyberattack by the BlackCat group. Local media report that following the attack, Wheat Ridge had to shut down its phones and email servers to assess the damage the cybercriminals had done to its network. That, in turn, prompted the city to close down City Hall to the public for more than a week. The cybercriminals demanded $5 million in Monero as the ransom, but the city declined to pay, opting to restore from backups. The city government has been able to return to normal business, and the attack is under investigation by the U.S. Federal Bureau of Investigation.

How It Could Affect Your Business: Ransomware attacks against governments and municipalities have been proliferating.

Rockstar Games
https://www.hackread.com/uber-hacker-rockstar-games-hacked-gta-6-data/

Exploit: Hacking

Rockstar Games: Video Game Developer

Risk to Business: 2.136 = Severe

Rockstar Games confirmed on Monday that a hacker broke into its systems and stole confidential internal data, including footage and source code from the previously unannounced next installment of its popular Grand Theft Auto series. The New York-based company appears to have been breached through a stolen employee Slack account. The hacker that claimed responsibility, “teapotuberhacker”, also says that they’re behind a murky hacking incident at Uber last week. The cybercriminal shared a link to footage and clips purportedly from Grand Theft Auto 6 on a Grand Theft Auto fan forum. The company has confirmed that the game is in development and that the attack occurred.

How It Could Affect Your Business: **T**his is a mess for Rockstar Games with a potentially nasty impact on the marketing and sales of a major new release that wasn’t ready for prime time yet.

New York Racing Association
https://www.bleepingcomputer.com/news/security/hive-ransomware-claims-attack-on-new-york-racing-association/

Exploit: Ransomware

New York Racing Association: Professional Group

Risk to Business: 2.703 = Moderate

The Hive ransomware operation has claimed responsibility for an attack on the New York Racing Association (NYRA). The NYRA operates the three major thoroughbred horse racing tracks in New York, the Aqueduct Racetrack, the Belmont Park (home of the Triple Crown event the Belmont Stakes) and the historic Saratoga Race Course. The attack took place in late August 2022 and breach notices were filed with authorities last week. Press reports say that the hackers have also published a link to freely download a ZIP archive containing all of the files they allegedly stole from NYRA's systems.

Risk to Individual: 2.624 = Major

Member data that may have been exposed includes Social Security numbers (SSNs), driver's license identification numbers, health records and health insurance information.

How it Could Affect Your Business: The involvement of health data could make this breach especially expensive and complicated.

American Airlines
https://www.bleepingcomputer.com/news/security/american-airlines-learned-it-was-breached-from-phishing-targets/

Exploit: Business Email Compromise

American Airlines: Airline

Risk to Business: 2.639 = Moderate

American Airlines has filed a breach notice declaring that it has had a data breach that may have impacted personal data for about 1700 customers and employees. Bleeping Computer detailed the incident saying that the American Airlines Cyber Security Response Team found out the attack from the targets of a phishing campaign that was using an employee's hacked Microsoft 365 account to send phishing messages. Reportedly, the attacker accessed multiple employees' accounts via phishing and used them to send more phishing emails to additional targets that have not been named.

Risk to Individual: 2.714 = Moderate

Employee or customer personal information exposed in the attack may have included employees' and customers' names, dates of birth, mailing addresses, phone numbers, email addresses, driver's license numbers, passport numbers or certain medical information.

How it Could Affect Your Business: Business email compromise can take many forms but it is always an expensive nightmare in the end.

LastPass
https://www.theregister.com/2022/08/25/lastpass_security/

Exploit: Ransomware

LastPass: Software Company

Risk to Business: 1.836 = Severe

Authentication software firm LastPass said on Thursday that someone broke into one of its developer's accounts and used that to gain access to proprietary data including source code. The company said in a statement that the incident had been contained and that they see no further evidence of unauthorized activity. LastPass says there is no evidence that customer data or encrypted password vaults were compromised. This breach may be related to the recent Twilio hack which impacted many companies.

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

How it Could Affect Your Business: The Information Technology sector was one of the 14 critical infrastructure sectors most victimized by ransomware last year.

Chester Upland School District
https://6abc.com/chester-upland-school-district-theft-13-million-stolen-from-delaware-county-attorney-jack-stollsteimer-fraud/12169001/

Exploit: Business Email Compromise

Chester Upland School District: Regional Education Authority

Risk to Business: 1.337 = Severe

A recent business email compromise attack on a Pennsylvania school district resulted in bad actors making off with more than $13 million. Authorities say hackers used a stolen district employee email account to snatch the money by sending official-looking messages from that account and then diverting payments to themselves. After diverting the payments, the cybercriminals then used a romance scam conducted through the dating site eHarmony to entice a Florida woman to launder the money unwittingly. The scheme came to light after the Pennsylvania Department of the Treasury flagged a large transfer, unraveling the whole mess. $10 million of the money has since been recovered.

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

How it Could Affect Your Business: Business email compromise is hard to detect but causes the most financial damage. This school district got lucky recovering money.

New Hampshire Lottery
https://www.wmur.com/article/new-hampshire-lottery-website-experiences-cyber-attack/41000488

Exploit: Hacking

New Hampshire Lottery: Gambling Program

Risk to Business: **2.809 = Moderate**

New Hampshire Lottery officials warned of a cyberattack on its website, cautioning players that people visiting the site should not click on any pop-up message. The site began to experience trouble early Friday morning, typically a busy day for lottery sales with the Mega Millions drawing taking place late Friday night. Officials said the site has been taken down as the matter is investigated and the trouble dealt with. They do not believe any personal data of players was stolen.

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

How it Could Affect Your Business: Cybercriminals love to exploit government-run websites to spread malware or for other nefarious purposes.