THE WEEK IN BREACH NEWS: 06/29/22 - 07/05/22

DenBe Computer Consulting
Connecting Business

July 6, 2022 by Dennis Jock

An insider incident causes trouble for OpenSea, cybercriminals claim to have scored data from AMD and ransomware stops the presses at Macmillan plus the importance of making sure that you are ready for a ransomware attack.

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***

Geographic Solutions Inc.
https://www.washingtonpost.com/politics/cyberattack-disrupts-unemployment-benefits-in-some-states/2022/06/30/8f8fe138-f88a-11ec-81db-ac07a394a86b_story.html

Exploit: Ransomware

Geographic Solutions Inc.: Software Company

Risk to Business: 1.742 = Severe

U.S. ambulance billing service Comstar has disclosed that it has exposed sensitive information belonging to medical patients. The company stated that it notices suspicious activity in March 2022, and an investigation determined that certain systems on Comstar's network were subject to unauthorized access, but investigators were ultimately unable to confirm what specific information on those systems was accessed.

How It Could Affect Your Business:: A data security incident at a service provider can be a disaster for any business and it will be especially damaging for the healthcare clients involved here.

.

California Department of Justice
https://www.theguardian.com/us-news/2022/jun/30/california-gun-owners-data-breach

Exploit: Human Error

California Department of Justice: State Government Agency

Risk to Business: 2.617 = Moderate

The California Department of Justice has disclosed a messy data breach courtesy of its Firearms Dashboard Portal. In the course of an update in late June, user data for anyone who had applied for a concealed carry firearms permit from 2011 through 2021 using the site was exposed for an estimated 24 hours in an unsecured spreadsheet. Data was also exposed on several other state-maintained gun-related online dashboards, including the Assault Weapon Registry, Handguns Certified for Sale, Dealer Record of Sale, Firearm Safety Certificate and Gun Violence Restraining Order dashboards.

Individual Risk: 2.613 = Moderate

User data that may have been exposed includes names, dates of birth, gender, race, driver license numbers, addresses, and criminal histories. Social Security numbers and financial information were not involved.

How It Could Affect Your Customers' Business: This will be an expensive employee mistake (and training failure) once regulators get finished with penalties for this incident.

Napa Valley Community College
https://napavalleyregister.com/news/local/ransomware-attack-caused-ongoing-napa-valley-college-internet-and-phone-system-outage/article_8bc46c5a-f410-11ec-bca2-e35eddc616de.html

Exploit: Ransomware

Napa Valley Community College: Institution for Higher Learning

Risk to Business: 1.601 = Severe

Napa Valley College has experienced a ransomware attack that resulted in its website and network systems being knocked offline. The incident, which started over two weeks ago, knocked systems including the college's on-campus telephones and employee email accounts out, leaving social media and an athletic department website run on a separate network as the only communication channels for the college. Professors and staff have since had email restored. The college also announced that it will continue teaching summer-session classes both in-person and remotely using an online platform that includes email and communication with professors. The incident is under investigation.

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

How It Could Affect Your Business: A data security incident at a service provider can be a disaster for any business and it will be especially damaging for the healthcare clients involved here.

.

OpenSea
https://techcrunch.com/2022/06/30/nft-opensea-data-breach/

Exploit: Insider Threat

OpenSea: Non-Fungible Token Marketplace

Risk to Business: 1.903 = Severe

NFT giant OpenSea has had a data breach caused by an employee at a third-party service provider misusing their access to data. OpenSea announced last week that an employee of email vendor Customer.io, misused their employee access to download and share email addresses of OpenSea's users and newsletter subscribers with an unauthorized external party. Customer.io told TechCrunch that the culprit was likely an employee who abused their role-specific access privileges and that no other company's data was involved in this incident.

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

How It Could Affect Your Business: Finance sector organizations have been at the top of the cybercriminal hit list, especially crypto-related entities.

.

New Peoples Bank
https://www.wvpublic.org/government/2022-07-01/security-breach-at-w-va-regional-bank-puts-customers-on-high-alert

Exploit: Hacking

New Peoples Bank: Financial Institution

Risk to Business: 2.304 = Severe

New Peoples Bank, a bank with branches in Virginia, West Virginia and Tennessee, has announced that it has experienced a data breach. An unauthorized person accessed bank systems on June 9, leading to data exposure for customers as well as disrupting banking and financial services. NPB is providing one year of free credit monitoring for those impacted.

Individual Impact: 2.383 = Severe

New Peoples Bank, a bank with branches in Virginia, West Virginia and Tennessee, has announced that it has experienced a data breach. An unauthorized person accessed bank systems on June 9, leading to data exposure for customers as well as disrupting banking and financial services.

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

How It Could Affect Your Business: Finance sector organizations have been at the top of the cybercriminal hit list, especially crypto-related entities.

Advanced Micro Devices (AMD)
https://www.securityweek.com/us-subsidiary-automotive-hose-maker-nichirin-hit-ransomware

Exploit: Hacking

Advanced Micro Devices (AMD): Semiconductor Company

Risk to Business: **2.822 = Moderate**

Chipmaker AMD is investigating a security breach after cybercrime gang RansomHouse, published a claim that they have obtained the company's data. claims to have breached AMD on January 5 to steal 450GB of data. The group claims to be targeting companies with weak security, boasting that it was able to compromise AMD due to the organization's weak passwords. In addition to the passwords, RansomHouse claims to have snatched network files and system information from AMD 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: Manufacturers aren't safe from cybercriminals looking to snatch information about operational technology.

.