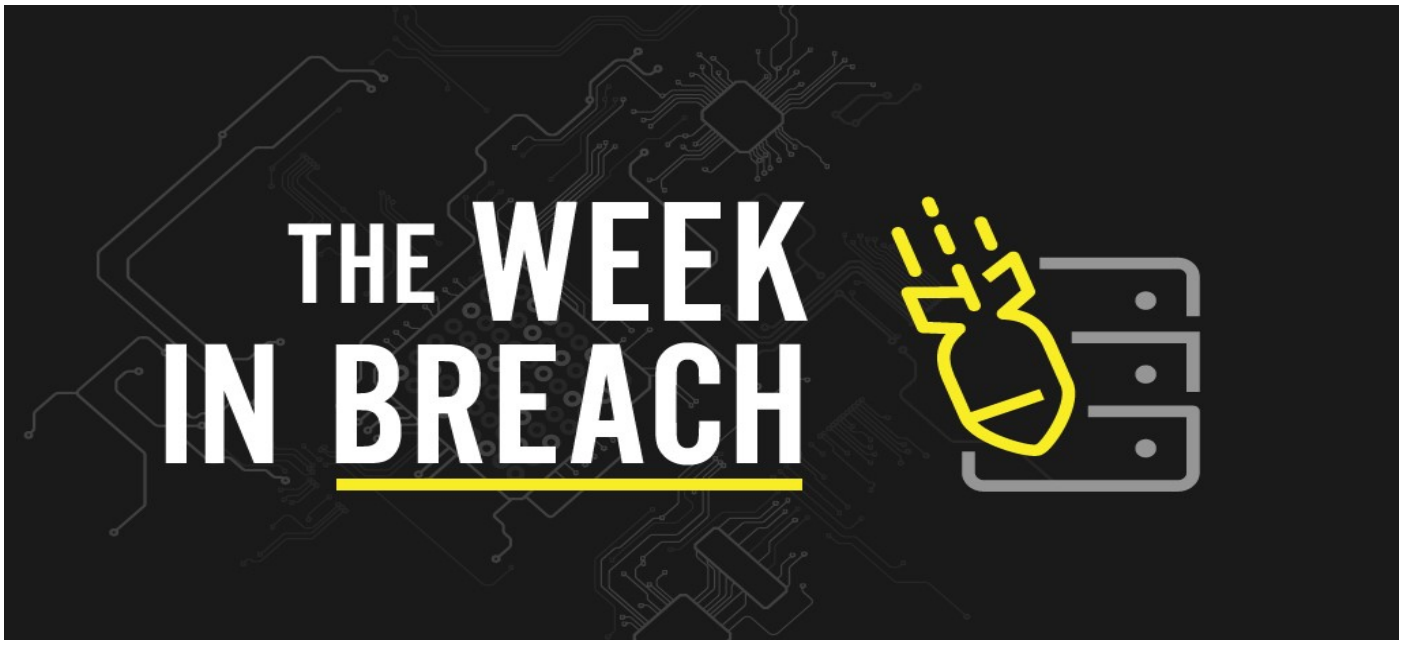
THE WEEK IN BREACH NEWS: 07/28/21— 08/03/21

DenBe Computer Consulting
Connecting Business

August 4, 2021 by Dennis Jock

Canada may have just had a Civic Holiday, but hackers aren't taking any time off as we show you in three Canadian breaches, plus hackers clearly have the cheat codes to beat security at EA, COVID-19 vaccination certifications have become a cybersecurity quagmire and the financial impact of a data breach (it goes deeper than you think).



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***

United States: Electronic Arts (EA)

https://therecord.media/hackers-leak-full-ea-data-after-failed-extortion-attempt/

Exploit: Hacking

Electronic Arts (EA): Video Game Maker

Risk to Business: **1.311 = Extreme**

Hackers have leaked an estimated 751GB of compressed EA data containing FIFA 21 source code on a dark web forum. Initially, they released a cache of 1.3GB of FIFA source code on July 14 as part of a demand for payment to stop them from releasing the rest, but after EA refused to play ball, the rest was added. According to reports, the hackers used the authentication cookies to mimic an already-logged-in EA employee's account and access EA's Slack channel and then tricked an EA IT support staffer into granting them access to the company's internal network, ultimately allowing them to download more than 780GB of source code from the company's internal code repositories. EA says that no player information was ever at risk and they've fixed the problem internally.

Customers Impacted: Unknown

How It Could Affect Your Business: Part of this hacking incident was powered by impersonation, which is a form of phishing, and is reminiscent of the 2020 Twitter hack that enabled cybercriminals to gain access to celebrity accounts by impersonating Twitter workers.

United States: University of San Diego Health

https://www.bleepingcomputer.com/news/security/uc-san-diego-health-discloses-data-breach-after-phishing-attack/

Exploit: Phishing

University of San Diego Health: Hospital System

Risk to Business: 1.663 = Severe

UC San Diego Health has disclosed a data breach after the compromise of some employees' email accounts. UC San Diego Health discovered that cybercriminals had gained access to some of its employees' email accounts through a phishing attack. The attackers may have accessed the personal information of patients, employees and students between December 2, 2020, and April 8, 2021.

Risk to Individual: 1.271 = Severe

Potentially impacted information includes: patients' full name, address, date of birth, email, fax number, claims information (date and cost of health care services and claims identifiers), laboratory results, medical diagnosis and conditions, Medical Record Number and other medical identifiers, prescription information, treatment information, medical information, Social Security number, government identification number, payment card number or financial account number and security code, student ID number and username and password. The hospital will offer free credit monitoring and identity theft protection services through Experian IdentityWorks for one year and is contacting impacted individuals via mail.

Customers Impacted: Unknown

How it Could Affect Your Business: Medical data is some of the hottest data to sell in dark web markets, earning cybercriminals a substantial profit and this hospital substantial fines under HIPAA and California Privacy regulations.

United States: City of Grass Valley, CA

https://sacramento.cbslocal.com/2021/07/29/grass-valley-cyberattack-ransom/

Exploit: Ransomware

City of Grass Valley, CA: Municipality

Risk to Business: 2.223=Severe

Municipalities have been ripe targets for cybercriminals, and they've scored another payday in Grass Valley, California. City services except emergency services experienced outages and the city ultimately chose to pay the ransom, citing data privacy concerns for its citizens. Grass Valley officials said the Federal Bureau of Investigation (FBI) was contacted. Several state agencies are still investigating. Services were restored after the ransom payment. Federal agencies including CISA and the FBI strongly discourage paying ransoms which is illegal in many circumstances.

Customers Impacted: Unknown

How it Could Affect Your Business: Cybercriminals have been striking municipalities and similar authorities frequently. Historically poor cybersecurity combined with a tendency to simply pay ransoms makes this a growth industry for cybercrime.

Canada: Calgary Parking Authority

https://calgaryherald.com/news/local-news/calgarians-personal-data-exposed-in-parking-authority-security-breach

Exploit: Misconfiguration

Calgary Parking Authority: Municipal Entity

Risk to Business: 1.705 = Severe

Calgary Parking Authority recently experienced a breach that exposed the personal information of vehicle owners. A misconfigured server containing computer-readable technical logs, payments, parking tickets, driver personal data and more was discovered in the wild by researchers. Reports say that the server, used to monitor the authority's parking system for bugs and errors, was left on the internet without a password in a security blunder.

Individual Risk: 1.622 = Severe

Data exposed includes drivers' full names, dates of birth, phone numbers, email addresses and postal addresses, as well as details of parking tickets and parking offenses, including license plates and vehicle descriptions, and in some cases the location data of where the alleged parking offense took place. The logs also contained some partial card payment numbers and expiry dates.

Customers Impacted: Unknown

How it Could Affect Your Business: It's hard enough to stay ahead of hackers without giving them an easy payday by making sloppy mistakes. Building a strong security culture is vital for keeping systems and data safe.

Canada: Homewood Health

https://bc.ctvnews.ca/unknown-number-of-british-columbians-personal-information-for-sale-online-after-health-company-extorted-1.5525715

Exploit: Nation-State Hacking

Homewood Health: Healthcare Provider

Risk to Business: **1.926 = Severe**

Ontario-based Homewood Health has disclosed that it fell victim to hacking earlier this year. The organization has begun contacting companies and agencies whose information may be compromised, including BC Housing, TransLink and the Provincial Health Services Authority. The organization is blaming the breach on the state-sponsored Chinese hackers Hafnium.

Individual Impact: There has not yet been confirmation that consumer personal or financial information has been compromised in this incident but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Cyberattacks against service providers have been steadily increasing as cybercriminals strike at lynchpins to gain access to even more valuable data.

Canada: D-Box

https://cyberintelmag.com/attacks-data-breaches/entertainment-company-d-box-recovers-from-ransomware-cyberattack/

Exploit: Ransomware

D-BOX: Gaming Specialty Electronics

Risk to Business: **1.919 = Severe**

Canadian immersive entertainment technology provider D-BOX said it was gradually resuming its activities following a ransomware attack. The company said it had worked with incident response experts to determine that the impact was limited to internal systems and that its services to studios and theatre operators were not affected. All services have now been restored. The company has stated that it believes that its policy of segmentation between internal and customer-focused systems helped protect its clients.

Individual Impact: There has not yet been confirmation that consumer personal or financial information has been compromised in this incident but the investigation is ongoing. There has not been any announcement that employee information was impacted however the company is offering identity theft protection to employees.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is the weapon of choice for both run-of-the-mill cybercriminals and nation state threat actors. Every business needs to be ready for it.

The Netherlands: Raven Hengelsport

https://www.theregister.com/2021/07/27/azure_blob_raven_hengelsport/

Exploit: Misconfiguration

Raven Hengelsport: Specialty Fishing Supply

Risk to Business: 1.602 = Severe

Dutch fishing supply specialist Raven Hengelsport left details of around 246,000 customers visible to anyone on a misconfigured Microsoft Azure cloud server for months. That server, hosting 18GB of company data covering at least 246,000 customers across 450,000 records, was discovered by security researchers and had purportedly been wide open for months. Even after researchers attempted to contact the company it took a long time for them to do anything about it.

Individual Risk: 2.416 = Moderate

The bonanza of information contained customer IDs, delivery dates, discounts, shipping fees, payments and shipment tracking numbers as well as PII like names, surnames, addresses, genders, phone numbers, email addresses and business names.

Customers Impacted: Unknown

How it Could Affect Your Business: Mistakes like this are only compounded by blunders in the response. It shows clients that you aren't concerned about their security if you aren't concerned about yours.

Indonesia: BRI Life

https://www.reuters.com/business/finance/indonesias-bri-life-probes-reported-data-leak-2-million-users-2021-07-27/

Exploit: Hacking

BRI Life: Insurer

Risk to Business: **2.802 = Moderate**

BRI Life, the insurance arm of Indonesia's Bank Rakyat Indonesia disclosed that it is investigating claims that the personal details of over two million of its customers were available in a dark web hacking forum. In a post on RaidForums, an unnamed user said they were selling a collection of 460,000 documents compiled from the user data of over two million BRI Life clients for $7,000.

Individual Risk: **2.802 = Moderate**

The user selling the data on RaidForums provided a video clip for proof that displayed bank account details, copies of Indonesian identification cards and taxpayer details. researchers estimate that 2 million people may have had PII exposed but information about specifics is hazy.

Customers Impacted: Unknown

How it Could Affect Your Business: Personal data like this is catnip for hackers because it sells quickly at a nice profit and retains value into the future.