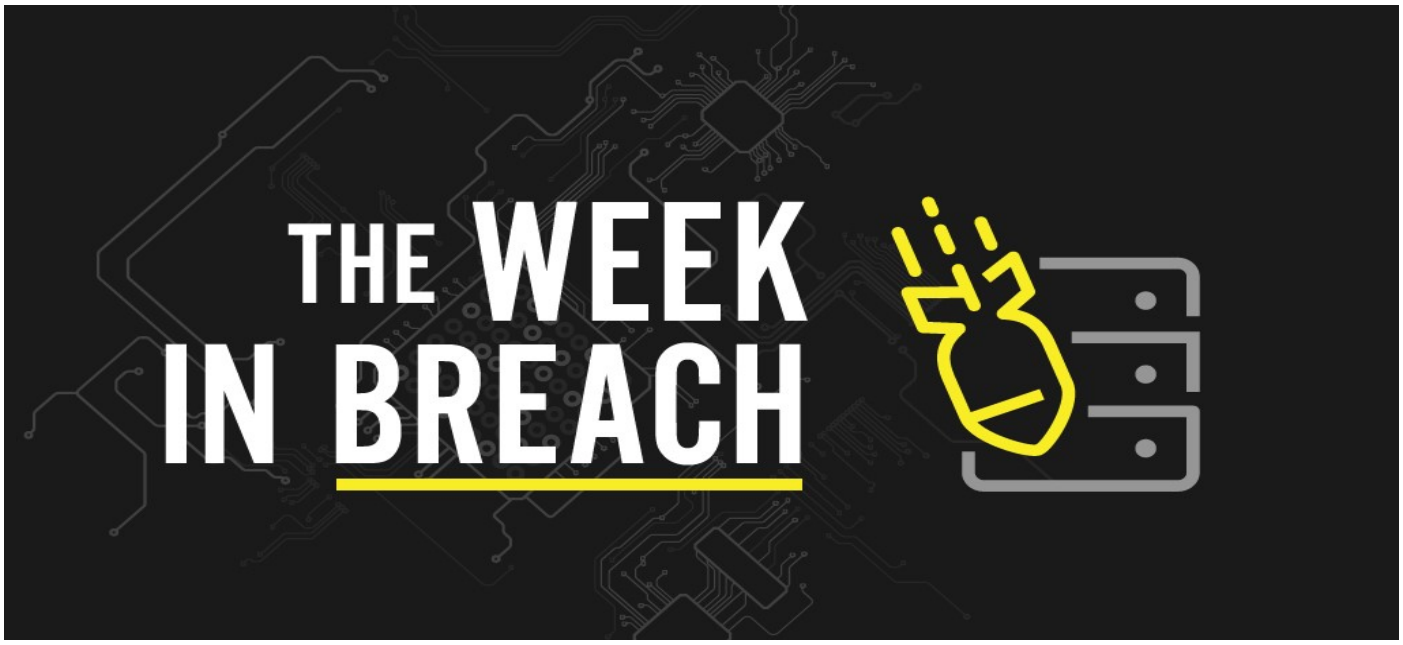
THE WEEK IN BREACH NEWS: 07/22/21— 7/27/21

DenBe Computer Consulting
Connecting Business

July 28, 2021 by Dennis Jock

Of course the Tokyo 2020 Games have already been hacked, ransomware at a South African port snarls maritime traffic, local governments feel the cyberattack squeeze and MIST joins the movement to adopt zero-trust security.



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: Florida Department for Economic Opportunity (DEO)

https://stpetecatalyst.com/zaps/floridas-deo-warns-of-unemployment-data-breach-affecting-nearly-58000/

Exploit: Hacking

Florida Department for Economic Opportunity (DEO): State Government Agency

Risk to Business: 2.550 = Severe

Records from more than 58,000 Florida unemployment accounts have been stolen in a data breach. The information was stolen in a suspected malicious insider incident, although details are sketchy. The stolen information was contained in the DEO's online unemployment benefit system, called CONNECT, and the records stolen fall between April 27 and July 16, 2021. The incident is still under investigation.

Individual Risk: 1.663= Severe

Exposed information includes social security numbers, bank account information and other personal details that users may have stored in CONNECT. The DEO purchased a year's subscription of LifeLock Identify protector services for all those affected.

Customers Impacted: 58,000

How It Could Affect Your Business: Personal data is the cybercriminal's bread and butter, especially when financial information is involved because it is quickly saleable in the busy dark web data markets.

United States: Yale New Haven Health

https://www.nbcconnecticut.com/news/local/your-information-may-have-been-compromised-in-yale-new-haven-healths-data-breach/2536460/

Exploit: Third-Party Data Breach

Yale New Haven Health: Medical System

Risk to Business: **1.716 = Severe**

Patients at Yale New Haven Health are being warned that their information has been stolen in an incident at a third-party vendor, Elekta. That company facilitates cancer treatments and was the victim of a ransomware attack just a few weeks ago that is rippling out to catch many medical institutions. Yale New Haven Health contends that hackers had no access to patient medical records, and a very small number of customers had financial information stolen.

Risk to Individual: **2.601 = Severe**

Officials said that certain demographic information such as names, addresses, phone numbers, emails, Social Security numbers, treatment locations and preferred languages were included in the Elekta databases impacted by the breach. A small group of people may have had their financial information exposed. Anyone with information that could have been exposed will be notified by mail and people who may have had their financial information exposed will be offered complimentary credit monitoring service.

Customers Impacted: 55,000

How it Could Affect Your Business: Medical data is some of the hottest product to sell in dark web markets, earning cybercriminals a substantial profit and this company a substantial HIPAA fine.

United States: Mobile County, Alabama

https://www.zdnet.com/article/guess-announces-breach-of-employee-ssns-and-financial-data-after-darkside-attack/

Exploit: Hacking

Mobile County, Alabama: Local Government

Risk to Business: 2.223=Severe

The Mobile County Commission has officially notified county employees of a computer system breach where employee data and sensitive information were at risk the county has announced that certain computer systems were subject to unauthorized access on May 24, 2021, culminating in employee information at risk. This is a developing situation as the investigation winds down. The county had initially stated that no sensitive information was exposed.

Individual Risk: 2.223=Severe

Mobile County alerted all employees, more than 1,600 people, that their information may have been exposed including Social Security numbers, dates of birth and other sensitive information. Also at risk, health insurance contract numbers for employees subscribed to receive health coverage and routing numbers for employees enrolled in direct deposit with the county.

Customers Impacted: Unknown

How it Could Affect Your Business: Even a small amount of data is attractive to data thieves who especially love vital information and financial data.

United Kingdom: Guntrader

https://www.theregister.com/2021/07/23/guntrader_hacked_111k_users_sql_database/

Exploit: Hacking

Guntrader: Gun Ownership Management System

Risk to Business: **1.705 = Severe**

Hackers hit a website used for buying and selling firearms in the UK making off with a 111,000-entry database containing partial information from a CRM product used by gun shops across the UK. The SQL database powered both the Guntrader.uk buy-and-sell website and its electronic gun shop register product, comprising about 111,000 users and dating between 2016 and 17 July this year. The Information Commissioner's Office was informed and an investigation is underway.

Individual Risk: **1.622 = Severe**

The database that the hackers scored provided a wealth of information about firearms enthusiasts in the UK including names, mobile phone numbers, email addresses, user geolocation data, and more including crypt-hashed passwords.

Customers Impacted: 111,000

How it Could Affect Your Business: Hackers are always in the market for fresh data, and this kind of information will net them a hefty profit fast.

Greece: Government of Thessaloniki

Exploit: Ransomware

Government of Thessaloniki: Municipal Government

Risk to Business: 1.302 = Extreme

Late last week, cybercriminals struck the government of Thessaloniki, Greece's second-largest city. The government was forced to shut down online applications and access at all municipal agencies. agencies were shut down over an electronic intrusion. Local officials confirmed that this was indeed a ransomware attack but did not specify the price. The incident is under investigation and services are in the process of being restored.

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 municipal governments, infrastructure and utilities have been steadily increasing, and organizations in those sectors need to step up their protection to stay safe.

South Africa: Transnet

https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/

Exploit: Hacking

Transnet: Port Authority

Risk to Business: 1.919 = Severe

A cyberattack at South Africa's biggest port operator, Transnet, has snarled maritime traffic around the world and left companies waiting for raw materials. The state-owned freight enterprise, comprised of shipping, railways and other logistics, has been forced to halt operations at container terminals in Durban, Ngqura, Port Elizabeth and Cape Town. The company has also placed many employees on leave. Transnet's Durban port handles 60% of the nation's shipments, including freight for other African nations. Officials said in a statement: "Transnet, including Transnet Port Terminals, experienced an act of cyberattack, security intrusion and sabotage, which resulted in the disruption of TPT normal processes and functions or the destruction or damage of equipment or information." some services are back up and running using limited, manual means. This incident remains under investigation.

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: This disruption is a massive blow to industries in Africa and around the world who need the raw materials and freight that Transnet handles.

Japan: Tokyo 2020 Olympics

https://www.computerweekly.com/news/252504456/Tokyo-2020-hit-by-data-breach

Exploit: Hacking

Tokyo 2020 Olympics: Sporting Event

Risk to Business: **2.719 = Moderate**

Just as the games were kicking off, officials disclosed that the usernames and passwords of Tokyo 2020 Olympic Games ticket holders and event volunteers were leaked online. The stolen credentials could be used to log on to websites for volunteers and ticket holders, compromising personal data such as names, addresses and bank account numbers.

Individual Risk: **2.416 = Moderate**

Officials are warning users of the Tokyo 2020 Games website for ticketing to change their usernames and passwords. No total numbers have been given on accounts exposed.

Customers Impacted: Unknown

How it Could Affect Your Business: This is hardly a surprise. Cybercriminals will nail every major event, and companies that work with event hosts need to be ready for trouble.