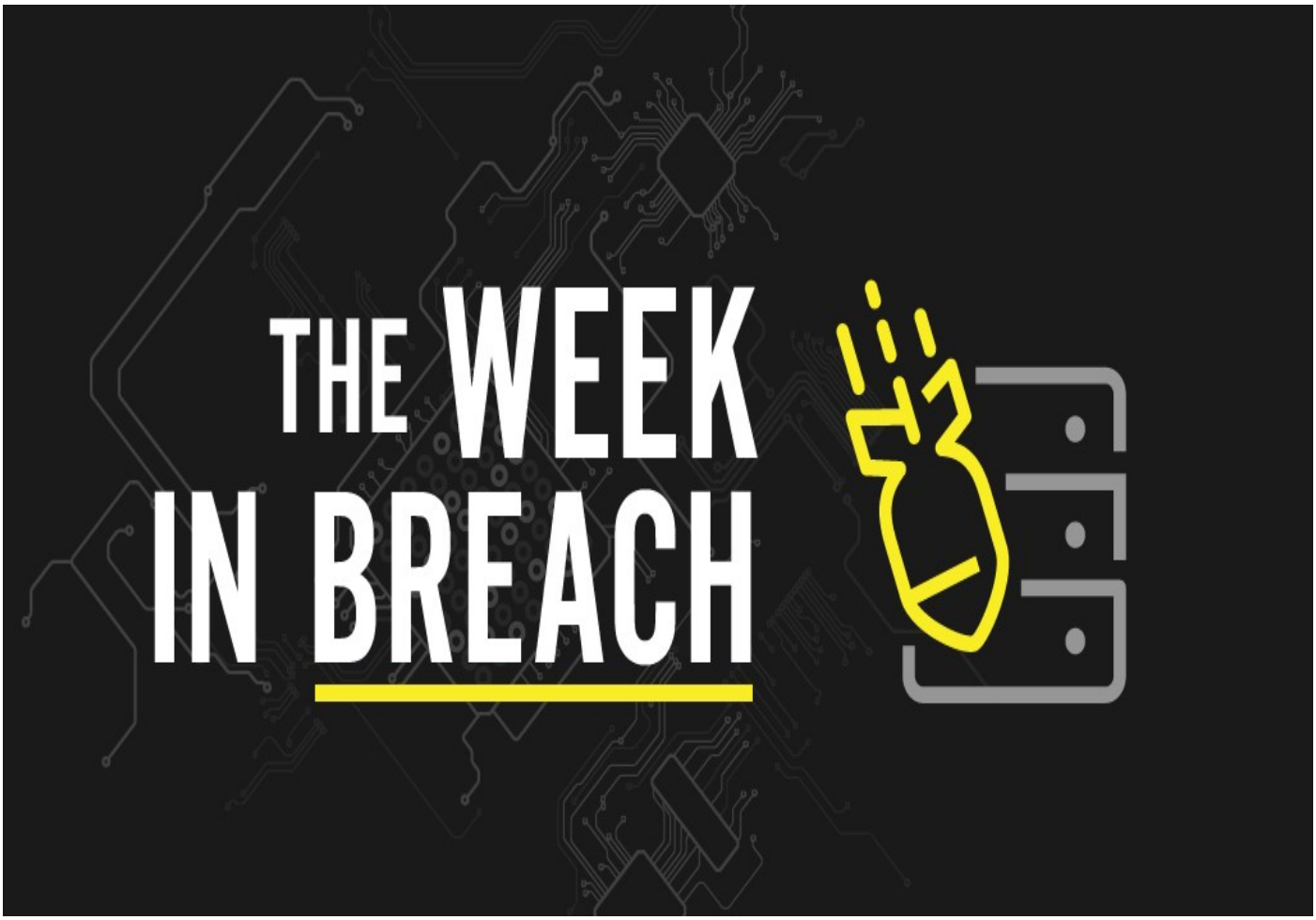
THE WEEK IN BREACH NEWS: 12/14/2022 - 12/20/2022

DenBe Computer Consulting
Connecting Business

December 21st, 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***

Sequoia
https://www.wired.com/story/sequoia-hr-data-breach/

Exploit: Hacking

Sequoia: Payroll & Benefits Management Company

Risk to Business: 2.176 = Severe

California-based major business services company Sequoia, known for their Sequoia One payroll services, has disclosed that they'd detected unauthorized access to one of the company's cloud storage repositories containing an array of sensitive and personal data. The company says it occurred between September 22 and October 6. The company noted that investigators from Dell SecureWorks did not find evidence of malware in its network and did not find any compromised computers or servers in Sequoia's infrastructure.

Risk to Business: 2.131 = Severe

Sequoia's breached cloud system stored an array of sensitive personal data, including names, addresses, dates of birth, gender, marital status, employment status, Social Security numbers, work email addresses, wage data related to benefits, and member IDs as well as any other ID cards, Covid-19 test results, and vaccine cards that individuals uploaded to the employment system.

How it Could Affect Your Business: Business services companies, especially those that store large amounts of sensitive data, are tempting targets for cybercriminals

Acuity Brands
https://www.securityweek.com/lighting-giant-acuity-brands-discloses-two-data-breaches

Exploit: Hacking

Acuity Brands: Lighting & Building Services

Risk to Business: 1.227 = Extreme

Acuity Brands has disclosed that it has had not just one but two previously unannounced data breaches in the last few years. The company says that it became aware of unauthorized access to its systems that resulted in data theft in early December 2021. While undertaking that investigation, Acuity also discovered that they'd had a separate, unrelated breach in October 2020, which also involved attempts to copy files from compromised systems. SecurityWeek said that they've found evidence that the 2021 attack may have been carried out by the notorious now-defunct Conti ransomware group. Acuity said that it had initially customers and partners about the breach in December 2021, and that this new notification is a follow-up for impacted employees. Employee data was accessed in both incidents. The company is likely facing a class-action lawsuit related to the incident in California.

Individual Risk: 1.207 = Extreme

In this incident, immigrants' names, case status, detention locations, and other information was published on a page where ICE regularly publishes detention statistics.

How it Could Affect Your Business: A cascade of damage can follow in the wake of a data breach, like expensive legal trouble.

The Metropolitan Opera
https://www.nytimes.com/2022/12/07/arts/met-opera-cyberattack-website.html/

Exploit: Hacking

The Metropolitan Opera: Arts Organization

Risk to Business: 1.981 = Severe

The Metropolitan Opera in New York City experienced a cyberattack that disrupted its ability to sell tickets. The company's website and box office were affected. The New York Times reported an outage of 30 hours. However, that didn't stop the show, with performances continuing as scheduled. There has been no announcement that this was a nation-state cyberattack, but the newspaper noted that The Met has been outspoken in its support for Ukraine throughout the Russia-Ukraine conflict, including parting ways with a leading Russian singer and hosting a benefit for Ukraine relief.

How It Could Affect Your Business: Bad actors love to hit businesses that are impacted by a time crunch in the hope of scoring a big payday.

The California Department of Finance
https://www.cyberscoop.com/lockbit-ransomware-california-department-of-finance/

Exploit: Ransomware

The California Department of Finance: Government Agency

Risk to Business: 1.981 = Severe

The LockBit 2.0 ransomware group says that it has snatched 76 gigabytes of data from the California Department of Finance. The agency has been added to the group's leak site with a deadline of December 24 to pay the unspecified ransom. The group claims that it has stolen a wide variety of data including databases, confidential data, financial documents and court records, providing seven screenshots of the data as proof. The California Governor's Office of Emergency Services did confirm that the California Cybersecurity Integration Center (Cal-CSIC) is actively investigating a cybersecurity incident at the agency but did not offer any further comment.

How It Could Affect Your Business: Government agencies are ripe ransomware targets because they maintain huge stores of often sensitive data.