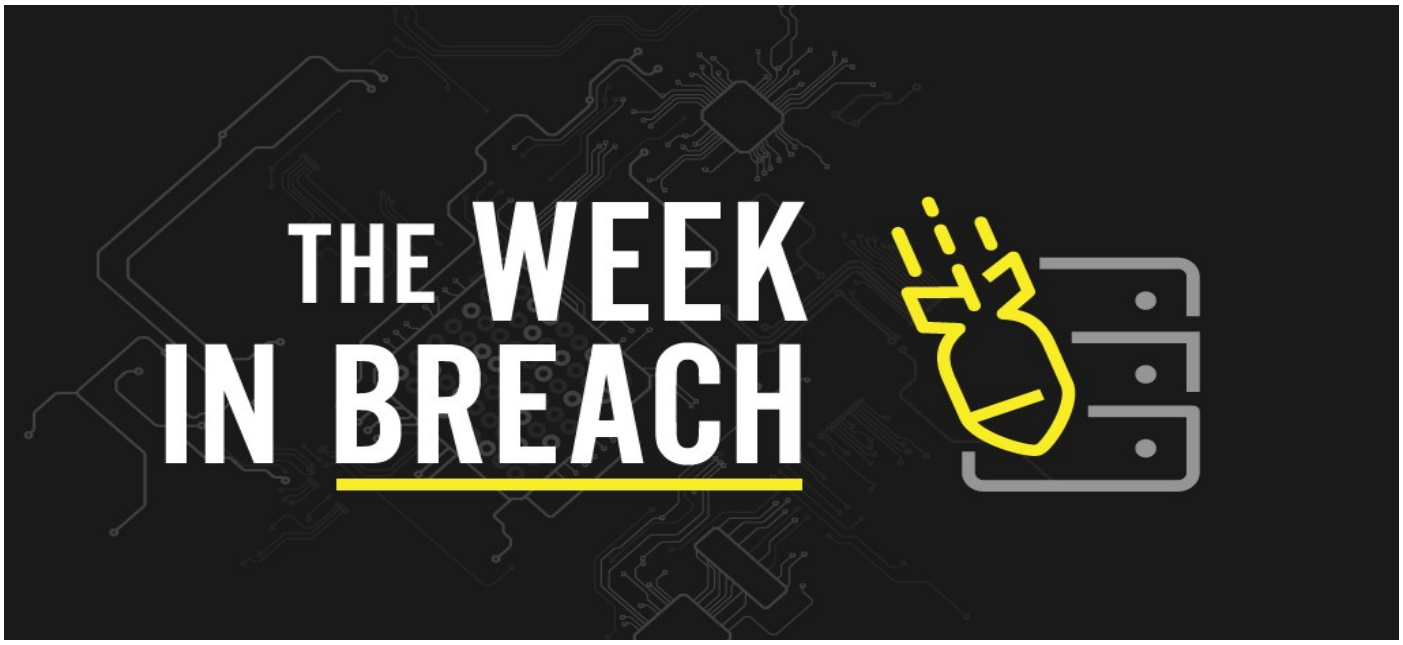
THE WEEK IN BREACH NEWS: 05/20/21—5/25/21

DenBe Computer Consulting
Connecting Business

May 26, 2021 by Dennis Jock

The spotlight is on supply chain risk and security blunders this week as we see the ripple effect of the Codecov and SITA supply-chain attacks continue, plus we'll dive into the new Verizon Data Breach Investigation Report for 10 things you need to see and give you an introduction to our new Nano Sessions!



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 – Utility Trailer Manufacturing

https://www.freightwaves.com/news/trailer-maker-utility-targeted-in-ransomware-attack

Exploit: Ransomware

Utility Trailer Manufacturing: Trailer Fabrication

Risk to Business: **1.655= Severe**

California-based Utility Trailer Manufacturing was hit by the Clop ransomware gang. As proof of the hit, the gang released 5 gigabytes of data to the dark web this week. The company has not been clear on the impact of the breach beyond saying that client data including payment records were not accessed and manufacturing remains normal.

Individual Risk: **1.507= Severe**

While the company is staying mum about the content of the breach, researchers have determined that an extensive amount of sensitive personal data about employees, including payrolls and human resources information was included in the incident after finding it on the dark web. Past and present employees should be alert for identity theft and spear phishing attempts.

Customers Impacted: Unknown

How It Could Affect Your Business: A new ransomware attack is launched every 40 seconds, and every business is in the line of fire. Making sure that you have all the bases covered and taking smart precautions like increased security awareness training can help reduce risk.

United States – Alaska Department of Health and Social Services

https://www.govinfosecurity.com/alaska-health-department-services-affected-by-malware-attack-a-16708

Exploit: Malware

Alaska Department of Health and Social Services: Regional Human Services Agency

Risk to Business: **1.833= Severe**

The Alaska health department's website was taken offline Monday evening and will be unavailable to the public for an indeterminate amount of time as IT teams work to investigate and recover from a malware attack. COVID-19 immunization and most data dashboards are maintained by an outside contractor and are still operational. The department's main website, background check system, the state of Alaska's vital records system, Alaska's behavioral health and substance abuse management system and the state's system for schools to report vaccine data to public health have all been impacted.

Individual Impact: No sensitive personal or financial information was confirmed as compromised in this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Malware that takes important systems offline can seriously impact an organization's operations, costing a fortune in remediation, investigation and recovery. Government targets have been especially appealing to cybercriminals due to their notoriously weak security.

United States – Bergen Logistics

https://www.hackread.com/logistics-giant-leaks-data-lolz-when-alerted/

Exploit: Unsecured Database

Bergen Logistics: Shipping & Fulfillment

Risk to Business: **2.812 = Moderate**

Security researchers recently discovered an exposed database belonging to Bergen Logistics. The Elasticsearch server contains a trove of 467,979 login credentials and shipment records relevant to the company's customers. Bergen Logistics handles import/export, picking and packing for clients in the fashion industry. the company also direct ships to customers of online marketplaces and e-commerce stores.

Individual Risk: **2.772= Moderate**

The exposed data for customers includes names, addresses, order numbers and details, email and contact information and plaintext passwords to customer accounts. This data could be used for spear phishing attempts.

Customers Impacted: Unknown

How it Could Affect Your Business: There are enough ways to suffer a cybersecurity incident without causing them through negligence, even though employee error is still the number one cause of a data breach. Making sure to cover the bases with basics goes a long way toward improving security.

United Kingdom - One Call

https://www.doncasterfreepress.co.uk/news/one-call-cyber-attack-all-you-need-to-know-about-hackers-darkside-and-insurance-boss-john-radford-3244076

Exploit: Ransomware

One Call: Insurer

Risk to Business: **1.606 = Severe**

Insurer OneCall admitted last week that a ransomware attack disrupted its core IT system and forced it to shut down its servers. The attack was perpetrated by the notorious DarkSide gang, which purportedly went dark after the Colonial Pipeline fiasco. the hackers are demanding a ransom of more than $20k. The company has released no clear information on what data was stolen or how long the investigation and recovery will take, although news outlets are reporting customer and financial data as potentially stolen by the gang.

Individual Impact: No confirmation is available as to whether sensitive personal or financial information was compromised in this incident and the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is the preferred weapon of cybercriminals, especially those in major gangs. Increased security awareness training is a must for every client because it makes organizations up to 70% less likely to experience damaging cybersecurity incidents like this one.

United Kingdom - FastTrack Reflex Recruitment

https://www.hackread.com/uk-recruitment-firm-exposed-applicants-data/

Exploit: Misconfiguration

FastTrack Reflex Recruitment: Staffing Firm

Risk to Business: **1.822 = Severe**

FastTrack Reflex Recruitment is the latest company to join the ranks of businesses that have had data leaks due to misconfigured AWS S3 buckets. The leaky bucket contained CVs for applicants and also included PII. Experts counted 21,000 client files (including duplicates), equating to 5GB of data.

Individual Risk: **1.780 = Severe**

In the bucket, applicant CVs were exposed including attached identity documents like passports, work permits, identity card numbers and similar documents. In many cases, names, addresses, social media profile

Customers Impacted: 21K applicants

How it Could Affect Your Business: Simple failures in setup like this are a symptom of low standards and a sloppy cybersecurity culture. They're also a quick way into disaster as this will not only cost money to fix, it will also incur penalties under GDPR and similar legislation.

Ireland - Ardagh Group

https://portswigger.net/daily-swig/packaging-vendor-ardagh-admits-cyber-attack-disrupted-operations

Exploit: Ransomware

Ardagh Group: Packaging Manufacturer

Risk to Business: **1.699 = Severe**

Glass and metal packaging giant Ardagh Group was snarled in a suspected ransomware attack. The company said that metal and glass packaging facilities remained operational, but the attack has caused shipping delays and interruptions. Investigation and remediation are underway, and the company expects to have everything back online by the end of the month.

Individual Impact: At this time, no sensitive personal or financial information was announced as compromised in this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Make sure your clients are taking every possible precaution against ransomware because 61% of organizations worldwide experienced a damaging ransomware incident in 2020.

New Zealand Waikato District Health Board

https://www.theregister.com/2021/05/19/new_zealand_hospitals_taken_down/

Exploit: Ransomware

Waikato District Health Board: Regional Healthcare Agency

Risk to Business: 1.115 = Extreme

Waikato District Health Board (DHB) had most of its IT services go offline Tuesday morning as the result of a suspect Conti ransomware attack, severely impacting services at six of its affiliate hospitals. Only email service has escaped the shutdown. With patient notes inaccessible, clinical services were disrupted and surgeries postponed. Phone lines went down and hospitals were forced to accept urgent patients only, using pencil and paper records. Service disruptions are expected to continue for several days.

Individual Impact: At this time, no sensitive personal or financial information was announced as compromised in this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Attacks on healthcare targets have been at the top of the cybercriminals playbook since the beginning of the global pandemic, and they represent a threat to public health, not to mention overstressing already burned-out hospital staffers.

India - Air India

https://www.bleepingcomputer.com/news/security/air-india-data-breach-impacts-45-million-customers/

Exploit: Third Party Data Breach

Toshiba: Electronics Manufacturer

Risk to Business: **2.001 = Severe**

Air India disclosed a data breach impacting 4.5 million of its customers following the hack of airline passenger service system provider SITA in February 2021. Dozens of airlines around the world had data exposed in that ransomware incident and the fallout is still shaking out. The airline confirmed that the breach involved personal data and credit card information registered between August 2011 and February 2021 by Air India or its subsidiaries.

Risk to Business: **2.113 = Severe**

The exposed data is reported to include passenger details like name, date of birth, contact information, passport information, ticket information, Star Alliance, and Air India frequent flyer data as well as credit card numbers.

Customers Impacted: Unknown

How it Could Affect Your Business: Third-party and supply chain data breaches like this one are becoming all too common as clever cybercriminals go for data-rich targets – and the problem will only get worse thanks to booming dark web data markets.

India - Domino's Pizza India

https://ciso.economictimes.indiatimes.com/news/user-info-linked-to-18cr-dominos-orders-leaked/82899181

Exploit: Hacking

Domino's Pizza India: Restaurant Chain

Risk to Business: 1.774 = Severe

Customer and employee information has been exposed in a hacking incident at Domino's Pizza India. Security researchers discovered 13TB of employee files and customer details exposed on the dark web. The data leak may be connected to another breach of the pizza chain earlier in April. Jubilant FoodWorks, operator of the chain, said that customers' financial information remains safe.

Risk to Business: 1.671 = Severe

It is unclear what if any payment data was snatched, but personal information for customers including order dates, addresses, names, order invoices and similar data is available. The hackers claim to also have employee data, but that is unconfirmed.

Customers Impacted: 180 million

How it Could Affect Your Customers' Business: Personal data is the most desirable information for cybercriminals right now, and every company needs to take precautions to keep them out of databases.

Japan—Mercari

https://www.bleepingcomputer.com/news/security/e-commerce-giant-suffers-major-data-breach-in-codecov-incident/

Exploit: Supply Chain Data Breach

Mercari: E-commerce Platform

Risk to Business: 1.922 = Severe

In another big supply chain hit this week, Japanese marketplace Mercari has been compromised as a result of the recent Codecov breach. earlier this year, code coverage tool Codecov disclosed that it had been a victim of a supply-chain attack that lasted for two months and allowed cybercriminals to meddle with its popular Bash Uploader, opening hundreds of companies up to risk. Mercari announced that tens of thousands of customer records, including financial information, were exposed to external actors due to the Codecov breach.

Individual Risk: 1.942 = Severe

In the final tally, 17,085 records related to the transfer of sales proceeds to customer accounts were exposed including bank code, branch code, account number, account holder (kana) and transfer amount; 7,966 records on business partners of “Mercari” and “Merpay,” including names, date of birth, affiliation, e-mail address, and other data were exposed. 2,615 records on employees were also impacted including those working for a Mercari subsidiary. The data is comprised of names of some employees as of April 2021, company email address, employee ID, telephone number, date of birth and other PII plus details of past employees, some contractors and employees of external companies who interacted with Mercari.

Customers Impacted: Unknown

How it Could Affect Your Business: Third-party data breaches like this one are the future of business. Reliance on outsourced service providers gives cybercriminals an easy way to scoop up data or snatch access credentials for multiple targets in one fell swoop.