TENNESSEE VOTERS
FOR ELECTION INTEGRITY

QUESTION: IF COMPANIES SPENDING MILLIONS OF DOLLARS CAN'T STOP A HACK, HOW CAN AN AGING VPN TECHNOLOGY KEEP OUR VOTE CENTER VOTING SAFE? ANSWER: IT PROBABLY CAN'T.

You'll most likely not hear much about this when the Williamson County Election Commission (WCEC) talks about their "convenience" vote centers – voting locations that are spread about the county to allow voters to vote in an election at any center they desire instead of voting in their nearby precinct.

An internet connection is required to service these vote centers. The connection is to help election workers check off citizens as they register to vote so the voter cannot vote hop… traveling to a second or third vote center to vote there after voting at the first one. This makes sense. And the WCEC is proud to affirm that a VPN protects the internet connection.

Vote centers have other serious security concerns, but the fact that there is an internet connection between each vote center that is barely protected by a VPN is probably one of the most frightening.

You see, the company that makes the VPN that WCEC uses was hacked in 2022. After spending millions of dollars on security, Cisco couldn't protect its own company. And they're supposed to be protecting our voting system? Check out this tech backgrounder that documents more facts about the current security issues of VPNs.

The same thing happened on October 5, 2023 in Washington D.C. as a cybercriminal group known as RansomedVC, which specializes in data extortion, targeted the D.C. Board of Elections, capturing more than 600,000 lines of D.C. voter data, including voter records (individual's name, registration ID, voter ID, partial Social Security number, driver's license number, date of birth, phone number, and email).

Using digital and paperless systems has made our lives much more convenient yet, in turn, has also made us incredibly vulnerable to those who can hack their way through our digital fortresses.

Data breaches have affected companies and organizations of all shapes, sizes, and sectors, and they're costing US businesses millions in damages. The widely-covered **T-Mobile data breach** that occurred in 2021, for instance, cost the company $350 million in 2022 – and that's just in customer pay outs. This puts more onus than ever on businesses to secure their networks, ensure staff have strong passwords and train employees to spot the telltale signs of phishing campaigns.

This document profiles just some of the data breaches that have occurred in 2022, 2023 and 2024 so far. Importantly, compare the cost of these business breaches in terms of how much these companies are spending – millions and billions of dollars -- to protect their data versus how much the WCEC spends against the potential of a Williamson County election being hijacked because of a hack or VPN intrusion. Pennies by comparison.

Check out the significant data breaches (and a couple of important data leaks) that have taken place since January 1, 2022, dated to the day they were first reported in the media.

If you're honest, we believe you'll conclude with us: It is imperative we move back to precinct voting and away from vote center voting and its required internet connection and weak VPNs. There's absolutely no guarantee that our system won't suffer a devastating hack. And with elections and our vote, you can't put the genie back in the bottle once that has happened. https://tech.co/news/data-breaches-updated-list

June 2024

June 1
Ticketmaster Data Breach: Ticketmaster confirms a rumored data breach from earlier in the year that saw records for its customers, including name, address, phone number, email address, order history and partial payment information, being offered for sale by hackers. Over 560 million customers are expected to be impacted.

May 2024

May 13
Helsinki City Council Data Breach: Local government systems in the Finnish capital Helsinki have suffered a data breach after a hack targeted at their education systems. Students and guardians may have had their personal information stolen from the system by a threat actor who managed to find a way in via a remote access server. The hack is known to have occurred at the beginning of the month, but that information was only made public by city officials this week.

May 10
JPMorgan Chase Data Breach: The Maine District Attorney's Office has been notified that almost half a million people banking with JPMorgan Chase could have had their personal information extracted from the company's systems thanks to a software flaw dating back to 2021. Luckily, at present, there seems to be no evidence of foul play or the data being misused in any manner. It could, however, have been accessed by authorized parties associated or working with the bank at the time.

May 9
Dell Data Breach: Dell emails customers to inform that that their data may have been compromised after an attack on its customer portal. According to Dell, while no financial information was accessed, customers' home addresses and order information may have been compromised. Data purportedly from the breach is being offered for sale on hacker forums, suggesting details of 49 million customers have been obtained.

May 1
Dropbox Data Breach: Dropbox tells users that its Dropbox Sign service has been accessed by a threat actor, who was able to see data including email addresses, phone numbers, hashed passwords and multi factor authenticator details. Dropbox cloud customers are unaffected.

April 2024

April 17
US Government Data Breach: A threat actor known to be part of a Serbian hacking group claims to have breached Space-eyes, CSO Online reports an intelligence corporation that works with the United States Department of Justice, the Department of Homeland Security, and a range of agencies and teams within the Armed Forces. The hacker claims they've stolen "highly confidential" documents relating to the services the company has provided to the government.

April 14
Giant Tiger Data Breach: A hacker claims to have stolen records of almost three million Giant Tiger customers. Although the attack happened back in March, the Canadian retailer only disclosed the incident this week. According to the hacker claiming to have extracted the data, the files contain email addresses, names, physical addresses and phone numbers.

April 12
Roku Data Breach: Streaming provider Roku has revealed that it suffered a data breach back in March. Over half a million (576,000) customers had their data compromised in the attack. "After concluding our investigation of this first incident" Roku explained in a blog post, referencing a previous data breach the company suffered this year. "We notified affected customers in early March and continued to monitor account activity closely to protect our customers and their personal information. Through this monitoring we identified a second incident, which impacted approximately 576,000 additional accounts."

March 2024

March 20
Vans Data Breach: Vans customers have been told they might be at risk of fraud and identity theft following a breach of the company's systems. "On December 13, we detected unauthorized activities on a part of our IT systems, apparently carried out by external threat actors," the company said in a breach notification letter sent out to account holders. It claims that no "detailed financial information" or passwords were exposed during the incident.

March 18
Fujistu Data Breach: Multinational technology company Fujitsu has confirmed that it fell victim to a cyberattack recently after malware was found on a collection of the company's work computers. The company – which employs almost 125,000 people globally – did not reveal what kind of information had been exposed by the attack.

February 2024

February 13
Bank of America Data Breach: Tens of thousands of Bank of America customers have had their data exposed in a breach relating to a ransomware attack targeted at Infosys McCamish Systems, one of the bank's service providers. The attack occurred at the beginning of November 2023. However, the news

only hit the headlines after notifications began to be sent around to customers at the start of February. This may have violated state laws determining how long companies have to notify impacted customers, some reports have pointed out. More than 57,000 customers are thought to have been impacted by the breach. Types of information exposed include addresses, names, social security numbers, DOBs, as well as some banking information (account numbers, credit card info).

January 2024

January 27
Anthropic Data Leak: Artificial intelligence startup Anthropic – the company behind the ChatGPT rival Claude – has suffered a small data leak. A contractor working with the company sent an email containing "non-sensitive customer information" to a third party who should not have had access to it.
Customer names and some information about their current Anthropic balances were the only types of information leaked in the incident, and customers impacted by the mistake have been notified.

January 23
Trello Data Breach: 15 million users of project management software platform Trello have their data leaked on the dark web, multiple sources report. "In January 2024, data was scraped from Trello and posted for sale on a popular hacking forum," a cautionary email from Have I Been Pawned warning users about the breach states. "Containing over 15 million email addresses, names, and usernames, the data was obtained by enumerating a publicly accessible resource using email addresses from previous breach corpuses" the email continues. "Trello advised that no unauthorized access had occurred."

January 2
Victoria Court System Data Breach: The Guardian reports that the court system in Victoria, Australia has been hacked – and the unauthorized parties gained access the recordings of various court hearings. However, "no other court systems or records, including employee or financial data, were accessed," chief executive Louise Anderson said in a statement.

December 2023

December 11
Norton Healthcare Data Breach: Norton Healthcare has suffered a data breach impacting an estimated 2.5 million people. The firm, based in Kentucky, says that threat actors gained unauthorized access to personal information about millions of patients, as well as a considerable number of employees.
The Healthcare provider is one of the biggest in the state, with more than 40 clinics dotted in and around Kentucky's state capital, Louisville, TechCrunch reports. Although the data breach happened between May 7 and May 9, it only came to light this month when it was filed with Maine's attorney general. An internal investigation by Norton suggests the threat actors had access to a broad selection of sensitive information.

November 2023

November 24
Vanderbilt University Medical Center Data Breach: A Tennessee-based medical institution has confirmed it fell victim to a ransomware attack orchestrated by the Meow ransomware gang. The Medical Center – which has over 40,000 employees – was one of several organizations added to the group leak database in November 2023. "Vanderbilt University Medical Center (VUMC) identified and contained a cybersecurity incident in which a database was compromised and has launched an investigation into the incident," the center revealed in a statement published by The Record. "Preliminary results from the investigation indicate that the compromised database did not contain personal or protected information about patients or employees."

November 15
Toronto Public Library Data Breach: The Toronto Public Library has said that sensitive, personal information relating to their employees, as well as library customers and volunteers, was stolen from their systems during a highly sophisticated ransomware attack. Some of the information had been stored in the system since 1998. According to Bleeping Computer, the Black Basta ransomware gang are behind the attack, a group whose activity were first observed in 2022.

November 5
Infosys Data Breach: Indian IT services company Infosys says they've been struck with a "security event" which made several of the firm's applications unavailable in its US unit, called Infosys McCamish Systems. The company is still investigating the impact the attack has had on its systems.

November 2
Boeing Data Breach: Aircraft manufacturer Boeing says that a "cyber incident" impacted several different elements of its business, with Reuters reporting that the company is already working with law enforcement to investigate the attack. The company has confirmed that the incident has no bearing on flight safety. The LockBit ransomware gang initially claimed responsibility for the attack and posted a threat directed at Boeing on their website – which has since been taken down. There is no clear evidence available at this point that suggests Boeing has paid the organization a ransom.

October 2023

October 30
Indian Council of Medical Research Data Breach: Around 815 million Indian citizens may have had their Covid test and other health data exposed to a huge data breach. A US security firm first alerted the Indian authorities in mid-October after a threat actor going by the name of "pwn0001" claimed to have the names, addresses, and phone numbers of hundreds of millions of Indians for sale. India's opposition parties are asking the government to urgently launch a probe into the breach and create a working data security plan for government agencies and departments.

October 19
Okta Data Breach: Identity services and authentication management provider Okta has revealed that its support case management system was accessed by a threat actor using stolen credentials. "The

unauthorized access to Okta's customer support system leveraged a service account stored in the system itself. This service account was granted permissions to view and update customer support cases" Okta's chief security office said in a recent statement.   "During our investigation into suspicious use of this account, Okta Security identified that an employee had signed in to their personal Google profile on the Chrome browser of their Okta-managed laptop."

October 11
Air Europa Data Breach: Spanish airline carrier Air Europa has told their customers to cancel all of their credit cards after hackers managed to access their financial information during a breach. Card numbers, expiration dates, and 3-digit CVV numbers found on the back of credit and debit cards were all extracted from the company's systems. Air Europa says the relevant authorities (including banks), have been notified and their systems are fully operational once more.

October 6
23andMe Data Breach: Biotech company 23andMe has suffered a data breach – customer accounts were broken into with a credential-stuffing attack. Genetic data belonging to people who have used the service has been stolen, which may include first names and last names, email addresses, birth dates, and information 23andMe stores relating to users' genetic ancestry and history. Reports suggest that the hackers were targeting/looking for data pertaining to individuals of Ashkenazi Jewish and Chinese descent.

September 2023

September 27
Hunter Biden Data Breach lawsuit: Hunter Biden – the son of US President Joe Biden – is suing both Rudy Guliani and his lawyer Robert Costello for accessing and sharing his personal information after they obtained his laptop from a computer repair shop. The lawsuit says that Guliani and Co. were responsible for a "total annihilation" of Hunter Biden's privacy.

September 25
SONY Data Breach: multinational technology company SONY has reportedly been broken into by ransomware group Ransomware.vc, who say they will sell the data they've stolen because SONY is refusing to pay them for it. Over 6,000 files have allegedly been extracted from the tech company's systems by the group, including build log and Java files.

September 25
Ontario Birth Registry Data Breach (MOVEit): Ontario's birth registry has confirmed that there has been a data breach of its systems, and around 3.4 million people who sought pregnancy care over the last ten years have had their information accessed. It is thought that more than two million babies born during this period have had their healthcare data exposed. it is one of the latest attacks to exploit the now well-known vulnerability in the MOVEit file transfer tool.

September 5
Topgolf Callaway Data Breach: US golf club manufacturer Topgolf Callaway has suffered a large data breach affecting over one million customers. Email notifications were sent out to those who were

affected this week. Data stolen includes full names, shipping addresses, email addresses, phone numbers, account passwords, and security question answers.

September 4
Freecycle Data Breach: Seven million Freecycle users have been affected in a breach of the nonprofit's systems. By the time the company had discovered that the breach had taken place, extracted data had already appeared on hacking forums. User IDs and email addresses were obtained during the breach, and Freecycle has advised all their members to reset their passwords as soon as possible.

August 2023

August 23
Duolingo data breach: Data pertaining to 2.6 million Duolingo users has been leaked on BreachForums. The data includes names, email addresses, phone numbers, social media information, as well as the languages that users were studying at the time of the breach.

August 11
IBM MOVEit data breach: 4.1 million patients in Colorado have had sensitive healthcare data stolen during another data breach exploiting a vulnerability in MOVEit transfer software. The systems affected are managed by tech behemoth IBM. Customers of Pension Benefit Information (PBI) and Genworth Life Insurance Company have additionally been notified that their data was affected by the breach.

August 8
Police Service of Northern Ireland data breach: Every police officer currently working in Northern Ireland has had their data compromised in what is being described as a "monumental" data breach. The data was leaked in error and mistakenly published while the service was responding to a Freedom of Information request. Surnames, initials, ranks, work locations, and departments of all of the police staff were leaked.

Missouri Medicaid data breach: Some recipients of Medicaid in Missouri have had their health information stolen. Like many recent data breaches, it seems the MOVEit transfer vulnerability was once again to blame. Information stolen may include names, dates of birth, possible benefit status, and medical claims information.

July 2023

July 27
Maximus data breach: US government contractor Maximus has suffered a huge data breach. Once again, hackers exploited the MOVEit transfer vulnerability and accessed health-related data pertaining to "at least 8 to 11 million" US citizens, the company said in an 8-K filing. A full review of the incident, the company says, will take "several more weeks".

July 24
Norwegian Government breach: Hackers have exploited a zero-day vulnerability in a third-party IT platform to hack into the government of Norway's systems. The country's authorities have shut down

email and mobile services for government employees in response. It is unclear at present who is behind the attack, but the vulnerability that they were exploiting has now been closed, the Norwegian Government said in a statement.

July 21
Roblox data breach: Almost 4,000 members of Roblox's developer community have had their data exposed in a leak, including phone numbers, email addresses, and dates of birth. The sensitive information, which belongs to individuals who attended Roblox developer conferences held between 2017 and 2020, was reportedly first lifted from Roblox's systems in 2021.

July 20
PokerStars data breach: The world's largest online poker platform has suffered a data breach exposing the information of 110,000 customers. The attackers – known as the Cl0p ransomware cartel – exploited a MOVEit zero-day vulnerability to gain access to the poker site's systems. PokerStars has confirmed that they're no longer utilizing the MOVEit transfer application after the incident. The stolen data consists of social security numbers, names, and addresses.

June 2023

June 27
American Airlines data breach: Hackers have reportedly stolen personal information relating to 'thousands' of pilots that applied for roles at American Airlines and Southwest Airlines. Rather than being taken directly from either airline, the information was extracted from a database maintained by a recruiting company. Around 8,000 pilots are thought to have been affected, including 2,200 represented by the Allied Pilots Association.

June 21
UPS Canada data breach: United Parcel Service has strongly hinted to customers based in Canada via a letter that their personal data may have been exposed in a breach, after fraudulent messages demanding payment before delivery were spotted. The strangely worded letter sent out to customers suggested that "a person who searched for a particular package or misused a package lookup tool" could have uncovered personal information relating to customers, such as phone numbers.

June 20
Bryan Cave/Mondelez data breach: Snack and confectionary manufacturer Mondelez, the parent company that owns Oreo, Chips Ahoy!, Sour Patch Kids, Toblerone, Milka, Cadbury, and many other well-known brands, has notified employees that their personal information has been compromised in a breach at law firm Bryan Cave. Bryan Cave provides Mondelez and a number of other large companies with legal services. According to the data breach notice filed to the Maine Attorney General's Office, 51110 employees are thought to have been affected. Although the data breach occurred in February of this year, it was only discovered three months later in May, the filing reveals.

June 19
Reddit data breach: Hackers purporting to be from the BlackCat ransomware gang have threatened Reddit with leaking 80GB of confidential data they stole from its servers in February. The gang is

demanding a $4.5 million payout and also wants Reddit to renege on its new pricing policy that garnered widespread backlash.

June 9
Intellihartx data breach: Healthcare management firm Intellihartx confirmed that hackers stole the medical details of over half a million patients, including social security numbers. According to a notice filed with the Maine attorney general's office, the breach took place in January, but wasn't discovered until April.

June 1
MOVEit hack, affecting Zellis, British Airways, BBC and others: MOVEit, a popular file transfer tool, was compromised, leading to sensitive data belonging to many firms that use the software being compromised as well. The hack was disclosed by Progress Software, makers of MOVEit, and since then, many companies have reported being affected. These include payroll provider Zellis, British Airways, BBC, and the province of Nova Scotia. However, it is believed that many more companies will have been impacted. Russian ransomware group Clop has claimed responsibility for the attack on June 6th.

May 2023

May 23
Apria Healthcare data breach: US healthcare company Apria Healthcare has told almost 1.9 million customers this week that their personal data may have been exposed during a data breach, The Register reports. The "unauthorized third party" access detected on "select Apria systems" referenced by the company in their notification apparently occurred in 2019 and again in 2021. Why the incident has only just been made public and was not declared earlier is unclear at present.

May 19
Suzuki data breach: Car manufacturer Suzuki had to halt operations at a plant in India after a cyberattack, reports this week have alleged. According to Autocar's sources, "production has been stalled since Saturday, May 10, and it is estimated to have incurred a production of loss of over 20,000 vehicles in this timeframe." The perpetrators of the attack have not been publicly identified by Suzuki.

May 16
PharMerica data breach: US Pharmaceutical giant PharMerica – which manages 2,500 different facilities across the US – has revealed that an unknown actor accessed its systems in March and extracted personal data pertaining to 5.8 million individuals (both alive and deceased). Social security numbers, birth dates, names, and health insurance information were all extracted from the Kentucky-based health provider's systems.

May 12
US Government data breach: Personal information pertaining to 237,000 US government employees has reportedly been exposed in a Department of Transport data breach. Reuters reports that the breached system is usually used to process "TRANServe transit benefits", which are effectively transport expenses that government employees commuting into offices can claim back. The Department of Transport told

Congress last week that it had “isolated the breach to certain systems at the department used for administrative functions”. No systems that deal with transportation safety have been affected.

May 1
T-Mobile data breach: T-Mobile has suffered yet another data breach, this time affecting around 800 of the telecom provider's customers. According to recent reports, customer contact information, ID cards, and/or social security numbers were scraped from PIN-protected accounts, as well as other personal information pertaining to T-Mobile customers. A data breach notification letter sent out to customers by T-Mobile, and subsequently published by Bleeping Computer, details the full extent of the data accessed by the threat actors. Unfortunately, this is the company's second data breach of the year. The first one, which took place in January, affected 37 million customers. T-Mobile was also breached in December 2021 and November 2022.

April 2023

April 10
Pizza Hut/KFC data breach: Yum! Brands, which owns fast food chains Pizza Hut, KFC, and Taco Bell, has informed a number of individuals that their personal data was exposed during a ransomware attack that took place in January of this year. The hospitality giant confirmed that names, driver's license, and ID card info was stolen. An investigation into whether the information has been used to commit fraud already is currently underway.

April 6
MSI data breach/Ransomware attack: Computer vendor Micro-Star International has suffered a data breach, with new ransomware gang Money Message claiming responsibility for the attack. The group says they've stolen 1.5TB of information from the Taiwanese company's systems and want $4 million in payment – or they'll release the data if MSI fails to pay. “Say [to] your manager, that we have MSI source code, including framework to develop bios, also we have private keys able to sign in any custom module of those BIOS and install it on PC with this bios,” a member of the ransomware gang said to an MSI agent in a chat seen by Bleeping Computer.

April 3
Western Digital data breach: Western Digital has reported a data breach, the scope of which at the time of writing is unknown. The company has stated that an unauthorized third party was able to access ‘a number' of cloud systems. Users of Western Digital products have reported being unable to access the cloud features of their devices since the hack was reported. In a statement on its site, Western Digital said it is “actively working to restore impacted infrastructure and services”, with more updates allegedly on the way.

March 2023

March 24
ChatGPT data leak: A bug found in ChatGPT's open-source library caused the chatbot to leak the personal data of customers, which included some credit card information and the titles of some chats they initiated. “In the hours before we took ChatGPT offline,” OpenAI said after the incident, “it was

possible for some users to see another active user’s first and last name, email address, payment address, the last four digits (only) of a credit card number, and credit card expiration date. Full credit card numbers were not exposed at any time.”

March 9
US House of Representatives data breach: A breach of a Washington DC-based healthcare provider that handles sensitive data belonging to a number of federal legislators and their families may have affected up to 170,000 people. The data has been put up for sale online, although the FBI is thought to have already purchased it as part of their investigation.

February 2023

February 21
Activision data breach: Call of Duty makers Activision has suffered a data breach, with sensitive employee data and content schedules exfiltrated from the company's computer systems. Although the breach occurred in early December 2022, the company has only recently revealed this to the public. According to reports, an employee's credentials were obtained in a phishing attack and subsequently used to infiltrate the system.

February 15
Atlassian Data Breach: Australian software company Atlassian seems to have suffered a serious data breach. A hacking group known as “SiegedSec” claims to have broken into the company's systems and extracted data relating to staff as well as floor plans for offices in San Francisco and Sydney. Included in the dataset are names, email addresses, the departments that staff work in, and other information relating to their employment at Atlassian. “THATS RIGHT FOLKS, SiegedSec is here to announce we have hacked the software company Atlassian,” the hacking group said in a message that was posted along with the data. “This company worth $44 billion has been owned by the furry hackers uwu.” Although Atlassian initially blamed software company office coordination platform Envoy for the breach, the company later reneged on this, revealing that the hacking group had managed to obtain “an Atlassian employee’s credentials that had been mistakenly posted in a public repository by the employee.”

February 10
Reddit data breach: Reddit has confirmed that the social media company suffered a data breach on February 5. “After successfully obtaining a single employee’s credentials” Reddit CTO Christopher Slowe explained in a recent statement regarding the attack, “the attacker gained access to some internal docs, code, as well as some internal dashboards and business systems.” Slowe said that Reddit's systems show “no indications of breach of our primary production systems (the parts of our stack that run Reddit and store the majority of our data),” but did confirm that “limited contact information… for company contacts and employees (current and former), as well as limited advertiser information” were all accessed. At present, Reddit has “no evidence to suggest that any of your non-public data has been accessed, or that Reddit’s information has been published or distributed online.”

February 8
Optus data breach extortion attempt: A man from Sydney has been served a Community Correction Order and 100 hours of community service for leveraging data from a recent Optus data breach to

blackmail the company's customers. Initially arrested back in October of last year, the perpetrator sent SMS communications to 92 people saying that their personal information would be sold to other hackers if they didn't pay AU$ 2000.

Weee! data breach: 1.1 million customers of Asian and Hispanic food delivery service Weee! have had their personal information exposed in a data breach. A threat actor that goes by the name of IntelBroker posted some of the leaked data on the infamous hacking forum Breached. However, Weee! told Bleeping Computer that "no customer payment data was exposed" because Weee! does not retain any payment information.

February 6
Sharp HealthCare data breach: Sharp HealthCare, which is the largest healthcare provider in San Diego, California, has notified 62,777 patients that their personal information was exposed during a recent attack on the organization's website. Social Security numbers, health insurance data, and health records belonging to customers have all been compromised, but Sharp says no bank account or credit card information was stolen.

January 2023

January 30
JD Sports data breach: As many as 10 million people may have had their personal information accessed by hackers after a data breach occurred at fashion retailer JD sports, which owns JD, Size?, Millets, Blacks, and Scotts. JD Sports CFO Neil Greenhalgh told the Guardian that the company is advising customers "to be vigilant about potential scam emails, calls, and texts" while also "providing details on how to report these."

January 19
T-Mobile data breach: T-Mobile has suffered another data breach, this time affecting around 37 million postpaid and prepaid customers who've all had their data accessed by hackers. The company claims that while it only discovered the issue on January 5th of this year, the intruders are thought to have been exfiltrating data from the company's systems since late November 2022. As discussed in the introduction to this article, this is not the first time that T-Mobile has fallen victim to a high-profile cyber-attack impacting millions of customers. In the aftermath of last year's attack, during which 76 million customers had their data compromised, the company pledged it would spend $150 million to upgrade its data security – but the recent attack raises serious questions over whether this has been well spent.

January 18
MailChimp breach: Another data breach for MailChimp, just six months after its previous one. MailChimp claims that a threat actor was able to gain access to its systems through a social engineering attack, and was then able to access data attached to 133 MailChimp accounts. It's a bad sign for the company, as the attack method is startlingly similar to last year's breach, casting serious doubts on its security protocols.

PayPal Data Breach: A letter sent to PayPal customers on January 18, 2023, says that on December 20, 2022, “unauthorized parties” were able to access PayPal customer accounts using stolen login credentials. PayPal goes on to say that the company has “no information” regarding the misuse of this personal information or “any unauthorized transactions” on customer accounts and that there isn't any evidence that the customer credentials were stolen from PayPal's systems.

January 6
Chick-fil-A data breach: Fast food chain Chick-fil-A is investigating “suspicious activity” linked to a select number of customer accounts. The company has published information on what customers should do if they notice suspicious activity on their accounts, and advised such customers to remove any stored payment methods on the account.

January 4
Twitter data breach: Twitter users' data was continuously bought and sold on the dark web during 2022, and it seems 2023 is going to be no different. According to recent reports, a bank of email addresses belonging to around 200 million Twitter users is being sold on the dark web right now for as little as $2. Even though the flaw that led to this leak was fixed in January 2022, the data is still being leaked by various threat actors.

December 2022

December 31
Slack security incident: Business communications platform Slack released a statement just before the new year regarding “suspicious activity” taking place on the company's GitHub account. “Upon investigation, we discovered that a limited number of Slack employee tokens were stolen and misused to gain access to our externally hosted GitHub repository. Our investigation also revealed that the threat actor downloaded private code repositories on December 27,” the company said. However, Slack confirmed that “no downloaded repositories contained customer data, means to access customer data, or Slack’s primary codebase”.

December 15
SevenRooms data breach: Threat actors on a hacking forum posted details of over 400GB of sensitive data stolen from the CRM platform’s servers. The information included files from big restaurant clients, promo codes, payment reports, and API keys. However, it seems that the servers that were breached did not store any customer payment details.

December 1
LastPass data breach: Password manager LastPass has told some customers that their information was accessed during a recent security breach. According to LastPass, however, no passwords were accessed by the intruder. This is not the first time LastPass has fallen victim to a breach of their systems this year – someone broke into their development environment in August, but again, no passwords were accessed.

November 2022

November 11
AirAsia data breach: AirAsia Group has, according to reports, suffered a ransomware attack orchestrated by "Daixin Team". The threat group told DataBreaches.net that they obtained "the personal data of 5 million unique passengers and all employees." This included name, date of birth, country of birth, location, and their "secret question" answer.

November 1
Dropbox data breach: Dropbox has fallen victim to a phishing attack, with 130 GitHub repositories copied, and API credentials stolen after credentials were unwittingly handed over to the threat actor via a fake CricleCI login page. However, Dropbox confirmed in a statement relating to the attack that "no one's content, passwords or payment information was accessed" and that the issue was "quickly resolved". Dropbox also said that they were in the process of adopting the "more phishing-resistant form" of multi-factor authentication technique, called "WebAuthn".

October 2022

October 26
Medibank data breach: Medibank Private Ltd, currently the largest health insurance provider in Australia, said today that data pertaining to almost all of its customer base (nearly 4 million Australians) had been accessed by an unauthorized party. The attack caused Medibank's stock price to slide 14%, the biggest one-day dip since the company was listed.

October 18
Vinomofo data breach: Australian wine dealer Vinomofo has confirmed it has suffered a cyber-attack. Names, dates of birth, addresses, email addresses, phone numbers, and genders of the company's almost 500,000 customers may have been exposed – although it is currently unclear how many have been affected.

October 17
MyDeal data breach: 2.2 million customers of Woolworths subsidiary MyDeal, an Australian retail marketplace, has been impacted by a data breach. According to reports, the company's CRM system was compromised, with names, email addresses, telephone numbers, delivery addresses, and some dates of birth exposed during the breach.

October 15
Shein data breach: Fashion brand Shein's parent company Zoetop has been fined $1.9 million for its handling of a data breach back in 2018, one which exposed the personal information of over 39 million customers that had made accounts with the clothing brand. The New York Attorney General's Office says Zoetop lied about the size of the breach, as the company initially said only 6.42 million accounts had been affected and didn't confirm credit card information had been stolen when it in fact had.

October 11
Toyota data breach: In a message posted on the company's website, the car manufacturer stated that almost 300,000 customers who had used its T-Connect telematics service had had their email addresses and customer control numbers compromised. The company assured customers that there was no danger of financial data such as credit card information, nor names or telephone numbers, having been breached. In its statement, Toyota acknowledged that the T-Connect database had been compromised since July 2017, and that customers should be vigilant for phishing emails.

October 10
Singtel data breach: Singtel, the parent company of Optus, revealed that "the personal data of 129,000 customers and 23 businesses" was illegally obtained in a cyber-attack that happened two years ago. Data exposed includes "National Registration Identity care information, name, date of birth, mobile numbers, and addresses" of breach victims.

October 7
Possible Facebook Accounts data breach: Meta said that it has identified more than 400 malicious apps on Android and iOS app stores that target online users with the goal of stealing their Facebook login credentials. "These apps were listed on the Google Play Store and Apple's App Store and disguised as photo editors, games, VPN services, business apps, and other utilities to trick people into downloading them," the Tech giant said.

October 3
LAUSD data breach: Russian-speaking hacking group Vice Society has leaked 500GB of information from The Los Angeles Unified School District (LAUSD) after the US's second-largest school district failed to pay an unspecified ransom by October 4th. The ransomware attack itself first made the headlines in early September when the attack disrupted email servers and computer systems under the district's control.

<u>September 2022</u>

September 23
Optus data breach: Australian telecoms company Optus – which has 9.7 million subscribers – has suffered a "massive" data breach. According to reports, names, dates of birth, phone numbers, and email addresses may have been exposed, while a group of customers may have also had their physical addresses and documents like driving licenses and passport numbers accessed.
The attackers are thought to be a state-sponsored hacking group or some sort of criminal organization and breached the company's firewall to get to the sensitive information. Australia's Information Commissioner has been notified. The Australian government has said Optus should pay for new passports for those who entrusted Optus with their data, and Prime Minister Antony Albanese has already suggested it may lead to "better national laws, after a decade of inaction, to manage the immense amount of data collected by companies about Australians – and clear consequences for when they do not manage it well."

September 20
American Airlines data breach: The personal data of a "very small number" of American Airlines customers has been accessed by hackers after they broke into employee email accounts, the airline has

said. Information accessed could have included customers' date of birth, driver's license, passport numbers, and even medical information, they added.

September 19
Kiwi Farms data breach: Notorious trolling and doxing website Kiwi Farms – known for its vicious harassment campaigns that target trans people and non-binary people – has been hacked. According to site owner Josh Moon, whose administrator account was accessed, all users should "assume your password for the Kiwi Farms has been stolen", "assume your email has been leaked", as well as "any IP you've used on your Kiwi Farms account in the last month".

Revolut data breach: Revolut has suffered a cyberattack that facilitated an unauthorized third party accessing personal information pertaining to tens of thousands of the app's clients. 50,150 customers have reportedly been impacted. The State Data Protection Inspectorate in Lithuania, where Revolut holds a banking license, said that email addresses, full names, postal addresses, phone numbers, limited payment card data, and account data were likely exposed.

September 18
Rockstar data breach: Games company Rockstar, the developer responsible for the Grand Theft Auto series, was victim of a hack which saw footage of its unreleased Grand Theft Auto VI game leaked by the hacker. In addition, the hacker also claims to have the game's source code and is purportedly trying to sell it. The breach is thought to have been caused through social engineering, with the hacker gaining access to an employee's Slack account. The hacker also claims to be responsible for the Uber attack earlier in the month. In a statement, Rockstar said: "We recently suffered a network intrusion in which an unauthorized third party illegally accessed and downloaded confidential information from our systems, including early development footage for the next Grand Theft Auto."

September 15
Uber data breach: Uber's computer network has been breached, with several engineering and comms systems taken offline as the company investigates how the hack took place. Dubbed a "total compromise" by one researcher, email, cloud storage, and code repositories have already been sent to security firms and The New York Times by the perpetrator. Uber employees found out their systems had been breached after the hacker broke into a staff member's slack account and sent out messages confirming they'd successfully compromised their network.

September 14
Fishpig data breach: Ecommerce software developer Fishpig, which over 200,000 websites currently use, has informed customers that a distribution server breach has allowed threat actors to backdoor a number of customer systems. "We are quite used to seeing automated exploits of applications and perhaps that is how the attackers initially gained access to our system" lead developer Ben Tideswell said of the incident.

September 7
North Face data breach: roughly 200,000 North Face accounts have been compromised in a credential stuffing attack on the company's website. These accounts included full names purchase histories, billing addresses, shipping addresses, phone numbers, account holders' genders, and XPLR Pass reward records.

No credit card information is stored on site. All account passwords have been reset, and account holders have been advised to change their passwords on other sites where they have used the same password credentials.

September 6
IHG/Holiday Inn data breach: IHG released a statement saying they became aware of "unauthorized access" to its systems. The company is assessing the "nature, extent and impact of the incident", with the full extent of the breach yet to be made clear.

September 3
TikTok data breach rumor: Rumors started circulating that TikTok had been breached after a Twitter user claimed to have stolen the social media site's internal backend source code. However, after inspecting the code, a number of security experts have dubbed the evidence "inconclusive", including haveibeenpwned.com's Troy Hunt. Users commenting on YCombinator's Hacker News, on the other hand, suggested the data is from some sort of ecommerce application that integrates with TikTok. Responding to a request for comment from Bloomberg UK, a spokesperson for TikTok said that the company's "security team investigated this statement and determined that the code in question is completely unrelated to TikTok's backend source code."

September 2
Samsung data breach: Samsung announced that they'd fallen victim to a "cybersecurity incident" when an unauthorized party gained access to their systems in July. In August, they learned some personal information was impacted, including names, contact information, demographics, birth dates as well as product registration information. Samsung is contacting everyone whose data was compromised during the breach via email.

August 2022

August 29
Nelnet Servicing data breach: Personal information pertaining to 2.5 million people who took out student loans with the Oklahoma Student Loan Authority (OSLA) and/or EdFinancial has been exposed after threat actors breached Nelnet Servicing's systems. The systems were compromised in June and the unauthorized party, who remained on the network until late July.

August 27
Facebook/Cambridge Analytica data breach settlement: Meta agreed on this date to settle a lawsuit that alleged Facebook illegally shared data pertaining to its users with the UK analysis firm Cambridge Analytica. The data was subsequently used by political campaigns in the UK and US during 2016, a year which saw Donald Trump become president and Britain leave the EU via referendum.

August 25
DoorDash data breach: "We recently became aware that a third-party vendor was the target of a sophisticated phishing campaign and that certain personal information maintained by DoorDash was affected," DoorDash said in a blog post. The delivery service went on to explain that "the information accessed by the unauthorized party primarily included [the] name, email address, delivery address and

phone number" of a number of DoorDash customers, whilst other customers had their "basic order information and partial payment card information (i.e., the card type and last four digits of the card number)" accessed.

LastPass breach: The password manager disclosed to its customers that it was compromised by an "unauthorized party". The company assured customers that this took place in its development environment and that no customer details are at risk. A September update confirmed that LastPass's security measures prevented customer data from being breached, and the company reminded customers that they do not have access to or store users' master passwords.

August 24
Plex data breach: Client-server media streaming platform Plex is enforcing a password reset on all of its user accounts after "suspicious activity" was detected on one of its databases. Reports suggest that usernames, emails, and encrypted passwords were accessed.

August 20
DESFA data breach: Greece's largest natural gas distributor confirmed that a ransomware attack caused an IT system outage and some files were accessed. However, a quick response from the organization's IT team – including deactivating online servers – meant that the damage caused by the threat was minimal.

August 10
Cisco data breach: Multi-national technology conglomerate Cisco confirmed that the Yanluowang ransomware gang had breached its corporate network after the group published data stolen during the breach online. Security experts have suggested the data is not of "great importance or sensitivity", and that the threat actors may instead be looking for credibility.

August 4
Twilio data breach: Messaging behemoth Twilio confirmed on this date that data pertaining to 125 customers was accessed by hackers after they tricked company employees into handing over their login credentials by masquerading as IT department workers.

July 2022

July 26
Uber data breach cover-up: Although this data breach actually took place way back in 2016 and was first revealed in November 2017, it took Uber until July 2022 to finally admit it had covered up an enormous data breach that impacted 57 million users, and even paid $100,000 to the hackers just to ensure it wasn't made public. The case will see Uber's former chief security officer, Joe Sullivan, stand trial for the breach – the first instance of an executive being brought to the dock for charges related to a data breach.

July 22
Twitter data breach: The first reports that Twitter had suffered a data breach concerning phone numbers and email addresses attached to 5.4 million accounts started to hit the headlines on this date, with the company confirming in August that the breach was indeed genuine. The vulnerability that

facilitated the breach was known by Twitter at the turn of the year and had been patched by January 13, 2022, so data theft must have happened within that short window.

July 19

Neopets data breach: On this date, a hacker going by the alias "TarTaX" put the source code and database for the popular game Neopet's website up for sale on an online forum. The database contained account information for 69 million users, including names, email addresses, zip codes, genders, and dates of birth.

July 18

Cleartrip data breach: Travel booking company Cleartrip – which is massively popular in India and majority-owned by Walmart – confirmed its systems had been breached after hackers claimed to have posted its data on an invite-only dark web forum. The full extent of the data captured from the company's internal servers is unknown.

July 13

Infinity Rehab and Avamere Health Services data breach: The Department of Health and Human Services was notified by Infinity Rehab that 183,254 patients had had their personal data stolen. At the same time, Avamere Health Services informed the HHS that 197,730 patients had suffered a similar fate. Information stolen included names, addresses, driver's license information, and more. On August 16, Washington's MultiCare revealed that 18,165 more patients were affected in the same breach.

July 12

Deakin University data breach: Australia's Deakin University confirmed on this date that it was the target of a successful cyberattack that saw the personal information of 46,980 students stolen, including recent exam results. Around 10,000 of the university's students received scam text messages shortly after the data breach occurred.

July 5

Marriot data breach: The Hotel group – which is no stranger to a data breach -- confirmed its second high-profile data breach of recent years had taken place in June, after a hacking group tricked an employee and subsequently gained computer access. According to databreaches.net, the group claimed to be in possession 20 GB of data stolen from the BWI Airport Marriott's server in Maryland. Marriot would be notifying 300-400 individuals regarding the breach.

June 2022

June 29

OpenSea data breach: NFT marketplace OpenSea – that lost $1.7 million of NFTs in February to phishers – suffered a data breach after an employee of Customer.io, the company's email delivery vendor, "misused their employee access to download and share email addresses provided by OpenSea users… with an unauthorized external party". The company said that anyone with an email account they shared with OpenSea should "assume they are affected".

June 17
Flagstar Bank data breach: 1.5 million customers were reportedly affected in a data breach that was first noticed by the company on June 2, 2022. “We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident” a letter from Flagstar bank to affected customers read.

June 14
Baptist Medical Center and Resolute Health Hospital data breach: The two health organizations – based in San Antonio and New Braunfels respectively – disclosed that a data breach had taken place between March 31 and April 24. Data lifted from its systems by an “unauthorized third party” included the social security numbers, insurance information, and full names of patients.

June 11
Choice Health Insurance data breach: On this date, Choice Health Insurance started to notify customers of a data breach caused by “human error” after it realized an unauthorized individual was offering to make data belonging to Choice Health available online. This had actually been publicly available since May 2022. The data dump consisted of 600MB of data with 2,141,006 files with labels such as “Agents” and “Contacts”.

June 7
Shields Health Care Group data breach: It was reported in early June that Massachusetts-based healthcare company Shields was the victim of a data breach that affected 2 million people across the United States. The breach was first discovered on March 28, 2022, and information such as Social Security numbers, Patient IDs, home addresses, and information about medical treatments was stolen. A class action lawsuit was filed against the company shortly after.

May 2022

May 26
Verizon data breach: A threat actor got their hands on a database full of names, email addresses, and phone numbers of a large number of Verizon employees in this Verizon data breach. Vice/Motherboard confirmed these numbers were legitimate by ringing the numbers contained in the databases and confirming they currently (or used to) work at Verizon. According to Vice, the hacker was able to infiltrate the system after convincing an employee to give them remote access in a social engineering scam.

May 23
Texas Department of Transportation data breach: According to databreaches.net, personal records belonging to over 7,000 individuals had been acquired by someone who hacked the Texas Dept. for Transportation.

May 20
Alameda Health System data breach: Located in Oakland, California, Alameda Health System notified the Department of Health and Human Services that around 90,000 individuals had been affected by a data breach after suspicious activity was detected on some employee email accounts, which was later

found to be an unauthorized third party.

May 17
National Registration Department of Malaysia data breach: A group of hackers claimed to hold the personal details of 22.5 million Malaysians stolen from myIDENTITI API, a database that lets government agencies like the National Registration Department access information about Malaysian citizens. The hackers were looking for $10,000 worth of Bitcoin for the data.

Cost Rican Government data breach: In one of the most high-profile cyberattacks of the year, the Costa Rican government – which was forced to declare a state of emergency – was hacked by the Conti ransomware gang. Conti members breached the government's systems, stole highly valuable data, and demanded $20 million in payment to avoid it being leaked. 90% of this data – amounting to around 670GB – was posted to a leak site on May 20.

May 7
SuperVPN, GeckoVPN, and ChatVPN data breach: A breach involving a number of widely used VPN companies led to 21 million users having their information leaked on the dark web, Full names, usernames, country names, billing details, email addresses, and randomly generated passwords strings were among the information available. **Unfortunately, this is not the first time supposedly privacy-enhancing VPNs have made the headlines for a data breach**.

April 2022

April 4
Cash App data breach: A Cash App data breach affecting 8.2 million customers was confirmed by parent company Block on April 4, 2022 via a report to the US Securities and Exchange Commission. The breach had actually occurred way back in December 2021, with customer names and brokerage account numbers among the information taken.

Emma Sleep data breach: First reported on April 4, customer credit card information was skimmed using a “Magecart attack”. “This was a sophisticated, targeted cyber-attack on the checkout process on our website and personal information entered, including credit card data, may have been stolen” an email to customers read.

March 2022

March 30
Apple & Meta data breach: According to Bloomberg, in late March, two of the world’s largest tech companies were caught out by hackers pretending to be law enforcement officials. Apple and Meta provided the threat actors with customer addresses, phone numbers, and IP addresses in mid-2021. The hackers had already gained access to police systems to send out fraudulent demands for the data. Some of the hackers were thought to be members of the Lapsus$ hacking group, who reportedly stole the Galaxy source code from Samsung earlier in the month.

March 26
US Department of Education data breach: It was revealed that 820,000 students in New York had their data stolen in January 2022, with demographic data, academic information, and economic profiles all accessed. Chancellor David Banks blamed software company Illuminate Education for the incident.

March 24
Texas Department of Insurance data leak: The state agency confirmed on March 24 that it had become aware of a "data security event" in January 2022, which had been ongoing for around three years. "Types of information that may have been accessible", the TDI said in a statement in March, included "names, addresses, dates of birth, phone numbers, parts or all of Social Security numbers, and information about injuries and workers' compensation claims. 1.8 million Texans are thought to have been affected.

March 18
Morgan Stanley client data breach: US investment bank Morgan Stanley disclosed that a number of clients had their accounts breached in a Vishing (voice phishing) attack in February 2022, in which the attacker claimed to be a representative of the bank in order to breach accounts and initiate payments to their own account. This was, however, not the fault of Morgan Stanley, who confirmed its systems "remained secure".

February 2022

February 25
Nvidia data breach: Chipmaker Nvidia confirmed in late February that it was investigating a potential cyberattack, which was subsequently confirmed in early March. In the breach, information relating to more than 71,000 employees was leaked. Hacking group Lapsus$ claimed responsibility for the intrusion into Nvidia's systems.

February 20
Credit Suisse data leak: Although this is technically a "data leak", it was orchestrated by a whistleblower against the company's wishes and one of the more significant exposures of customer data this year. Information relating to 18,000 Credit Suisse accounts was handed over to German publication Süddeutsche Zeitung, and showed the Swiss company had a number of high-profile criminals on their books. The incident kickstarted a fresh conversation about the immorality of Switzerland's banking secrecy laws.

January 2022

January 20
Crypto.com data breach: On January 20, 2022, Crypto.com made the headlines after a data breach led to funds being lifted from 483 accounts. Roughly $30 million is thought to have been stolen, despite Crypto.com initially suggesting no customer funds had been lost.

January 19

Red Cross data breach: In January, it was reported that the data of more than 515,000 “extremely vulnerable” people, some of whom were fleeing from warzones, had been seized by hackers via a complex cyberattack. The data was lifted from at least 60 Red Cross and Red Crescent societies across the globe via a third-party company that the organization uses to store data.

January 6

Flexbooker data breach: On January 6, 2022, data breach tracking site HaveIBeenPwned.com revealed on Twitter that 3.7 million accounts had been breached in the month prior. Flexbooker only confirmed that customer names, phone numbers, and addresses were stolen, but HaveIBeenPwned.com said “partial credit card data” was also included. Interestingly, 69% of the accounts were already in the website’s database, presumably from previous breaches.

Data Breaches vs Data Leaks vs Cyberattacks

This article largely concerns data breaches. A data breach occurs when a threat actor breaks into (or breaches) a company, organization, or entity’s system and purposefully lifts sensitive, private, and/or personally identifiable data from that system. When this happens, companies are sometimes forced to pay ransoms, or their information is stolen ad posted online. According to one estimate, 5.9 billion accounts were targeted in data breaches last year (2022).

This is different from a data leak, which is when sensitive data is unknowingly exposed to the public/members of the public, such as the Texas Department for Insurance leak mentioned above. The term “data leak” is often used to describe data that could, in theory, have been accessed by people it shouldn't of, or data that fell into the hands of people via non-malicious means. A government employee accidentally sending someone an email with sensitive data is usually described as a leak, rather than a breach.

Although all data breaches fall under the umbrella of a “cyberattack“, cyberattacks are not limited to data breaches. Some cyber-attacks have different motivations – such as slowing a website or service down or causing some other sort of other disruption. Not all cyberattacks lead to the exfiltration of data, but many do.

###

https://tech.co/news/data-breaches-updated-list