



NATIONAL DATA RESILIENCE BRIEFING • 50 STATES + D.C.

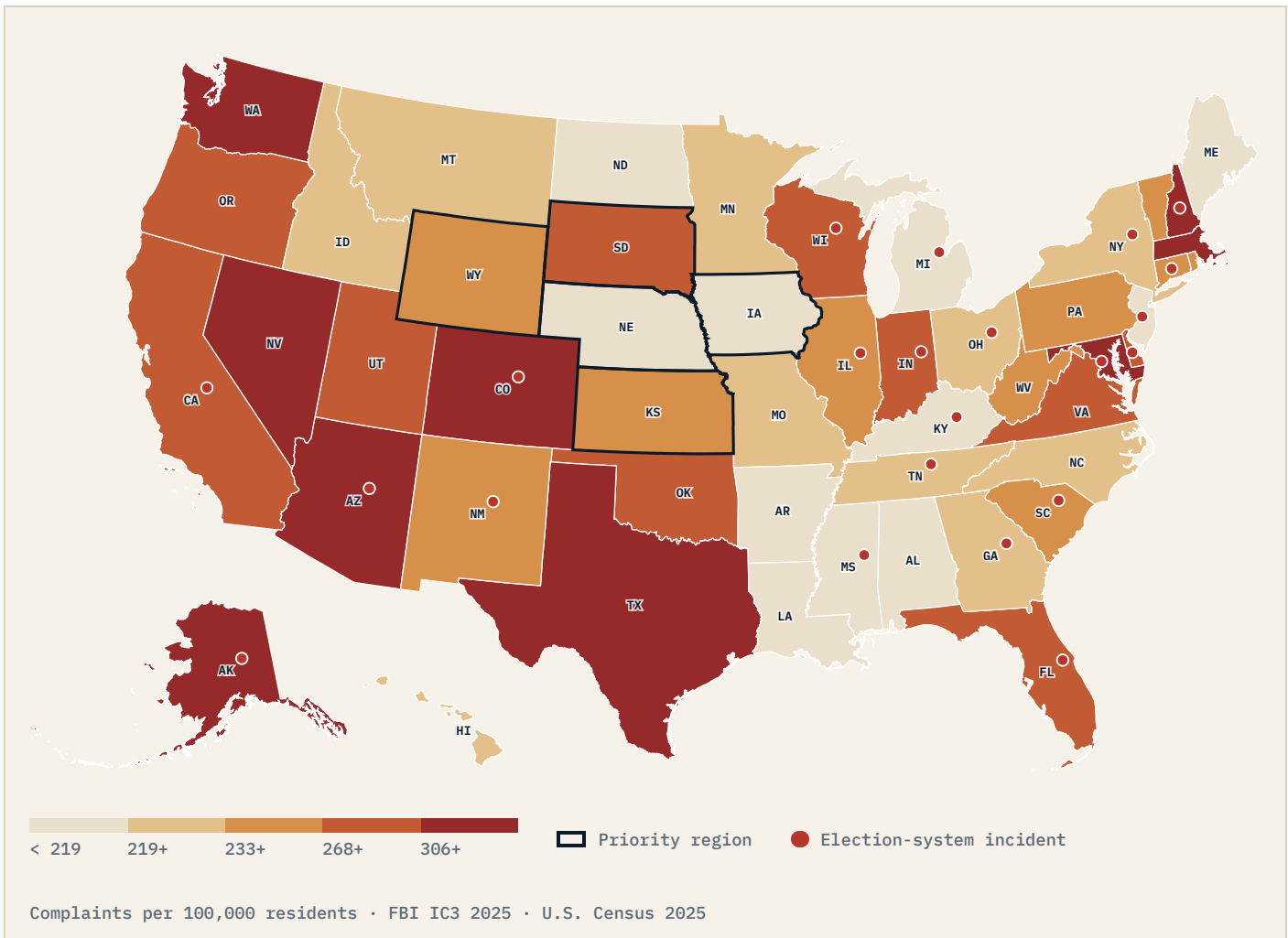
See the threat. *Protect the public record.*

FBI cybercrime exposure in all 51 jurisdictions, the documented public-sector incidents behind it, and the plan to harden election and government records.

Every jurisdiction is exposed

Americans filed more than a million cybercrime complaints with the FBI in 2025. Election offices, courts, state agencies, counties and schools in every region have been breached, extorted or knocked offline.

1,008,597 Cybercrime complaints filed with the FBI in 2025	\$20.9B Reported losses in 2025, the highest on record	51 Jurisdictions profiled: every state and D.C.	102 Documented public-sector incidents across all 51 jurisdictions
--	--	---	--



No state is out of range

Iowa has the lowest complaint rate in the country and still logged 168 per 100,000 residents. The national figure is about 295.

Hot spots run coast to coast

D.C., Alaska, Nevada, Arizona and Massachusetts lead on complaints per resident. California, Texas and Florida lead on total losses.

Election systems are a target

24 of the documented incidents hit election systems directly, in 22 jurisdictions, from voter databases to results websites.

How every state compares

Ranked by cybercrime complaints per 100,000 residents, 2025. Rank 1 is the highest rate. Priority region shaded.

RANK	JURISDICTION	REGION		PER 100K	COMPLAINTS	LOSSES	LOSS / RESIDENT	INCIDENTS
1	District of Columbia	South	<div></div>	448.8	3,113	\$97.4M	\$140.37	2
2	Alaska	West	<div></div>	434.3	3,202	\$40.0M	\$54.22	2
3	Nevada	West	<div></div>	407.2	13,366	\$302.2M	\$92.08	2
4	Arizona	West	<div></div>	378.7	28,868	\$630.7M	\$82.73	2
5	Massachusetts	Northeast	<div></div>	320.6	22,936	\$410.9M	\$57.44	2
6	Washington	West	<div></div>	320.2	25,619	\$458.2M	\$57.26	2
7	Colorado	West	<div></div>	313.5	18,847	\$355.0M	\$59.05	2
8	Maryland	South	<div></div>	310.1	19,430	\$390.2M	\$62.29	2
9	New Hampshire	Northeast	<div></div>	309.0	4,374	\$59.3M	\$41.89	2
10	Texas	South	<div></div>	308.8	97,912	\$1.83B	\$57.57	2
11	Florida	South	<div></div>	306.2	71,843	\$1.60B	\$68.03	2
12	Indiana	Midwest	<div></div>	297.9	20,777	\$233.0M	\$33.42	2
13	California	West	<div></div>	295.8	116,414	\$3.67B	\$93.37	2
14	Oregon	West	<div></div>	292.0	12,477	\$193.2M	\$45.21	2
15	Delaware	South	<div></div>	291.4	3,089	\$62.0M	\$58.51	2
16	Oklahoma	South	<div></div>	290.2	11,964	\$131.9M	\$31.99	2
17	Virginia	South	<div></div>	285.1	25,314	\$476.1M	\$53.62	2
18	Utah	West	<div></div>	279.8	9,903	\$195.4M	\$55.22	2
19	Wisconsin	Midwest	<div></div>	279.3	16,680	\$194.2M	\$32.52	2
20	South Dakota	Midwest	<div></div>	268.8	2,514	\$51.5M	\$55.02	2
21	New Mexico	West	<div></div>	267.6	5,688	\$85.6M	\$40.26	2
22	Kansas	Midwest	<div></div>	266.3	7,927	\$147.3M	\$49.49	2
23	South Carolina	South	<div></div>	263.9	14,699	\$264.1M	\$47.41	2
24	Wyoming	West	<div></div>	263.6	1,552	\$25.8M	\$43.87	2
25	Connecticut	Northeast	<div></div>	263.4	9,714	\$219.5M	\$59.51	2
26	Illinois	Midwest	<div></div>	259.3	32,977	\$535.3M	\$42.08	2
27	Vermont	Northeast	<div></div>	245.1	1,580	\$26.6M	\$41.21	2
28	Rhode Island	Northeast	<div></div>	242.3	2,700	\$72.0M	\$64.57	2
29	Pennsylvania	Northeast	<div></div>	238.6	31,154	\$537.8M	\$41.18	2
30	West Virginia	South	<div></div>	238.3	4,209	\$92.6M	\$52.46	2
31	Minnesota	Midwest	<div></div>	233.2	13,595	\$248.9M	\$42.69	2
32	Hawaii	West	<div></div>	232.3	3,328	\$106.4M	\$74.29	2

RANK	JURISDICTION	REGION	PER 100K	COMPLAINTS	LOSSES	LOSS / RESIDENT	INCIDENTS
33	Ohio	Midwest	 232.1	27,626	\$421.3M	\$35.40	2
34	North Carolina	South	 231.6	25,940	\$431.6M	\$38.54	2
35	Georgia	South	 229.5	25,936	\$534.6M	\$47.30	2
36	Montana	West	 228.7	2,618	\$53.2M	\$46.47	2
37	New York	Northeast	 226.2	45,255	\$1.23B	\$61.31	2
38	Missouri	Midwest	 224.7	14,087	\$233.9M	\$37.31	2
39	Tennessee	South	 222.3	16,261	\$269.2M	\$36.80	2
40	Idaho	West	 220.7	4,479	\$88.7M	\$43.71	2
41	Michigan	Midwest	 219.1	22,191	\$381.1M	\$37.63	2
42	New Jersey	Northeast	 216.2	20,648	\$660.4M	\$69.17	2
43	Kentucky	South	 204.3	9,414	\$119.7M	\$25.98	2
44	Maine	Northeast	 204.1	2,888	\$56.5M	\$39.96	2
45	Arkansas	South	 197.8	6,161	\$102.5M	\$32.92	2
46	Alabama	South	 191.3	9,936	\$167.2M	\$32.20	2
47	Louisiana	South	 186.7	8,623	\$105.4M	\$22.83	2
48	Nebraska	Midwest	 184.5	3,724	\$71.8M	\$35.60	2
49	North Dakota	Midwest	 177.4	1,418	\$37.9M	\$47.37	2
50	Mississippi	South	 172.1	5,084	\$77.4M	\$26.19	2
51	Iowa	Midwest	 167.9	5,436	\$95.5M	\$29.50	2

What has already happened

Documented cyber incidents against election offices, courts, state agencies, counties, schools and public health systems, newest first.

DATE	JURISDICTION	INCIDENT	SCALE • SOURCE
2026			
Oct 2026	Mississippi	Ransomware forces Vicksburg to shut down city systems A ransomware attack forced Vicksburg to temporarily shut down city computer systems, affecting utility payment systems. Emergency services were not affected, and the city was investigating with the FBI and DHS.	City systems shut down The Record
Sep 2026	Wyoming PRIORITY	Court vendor breach exposes Wyoming court users' personal data The Wyoming Judicial Branch said on Sept. 2, 2026, that court user data was obtained in a breach at its vendor, West Publishing Corporation, which also hit other court systems around the country. Names, addresses and dates of birth of people who dealt with district courts or the Supreme Court from 2015 to 2025 were compromised, and courts kept operating normally.	Court users, 2015-2025 Wyoming Public Media
Aug 2026	South Dakota PRIORITY	Cyberattack hits part of Mitchell city computer network An August 2026 cyberattack hit part of the City of Mitchell's computer network and affected a small number of employees. Forensic specialists recovered files, systems returned to normal shortly after, and officials said they saw no sign the data was misused.	Small number of employees Dakota News Now
Jul 2026	South Dakota PRIORITY	Pennington County, S.D., systems knocked out A cyberattack took down Pennington County's computer systems and cut off some services for residents. Mitchell's city hall was also disrupted, and Rapid City's water system was targeted, though officials said its network was not accessed.	County + city services South Dakota Searchlight
Jun 2026	District of Columbia	Cyberattack compromises D.C. Housing Authority systems, website down On June 29, 2026, the D.C. Housing Authority was hit by a cyberattack that left its systems compromised, took its website offline and cut staff off from their files. It was not clear whether any personal information was exposed.	Agency website, files offline WJLA 7News
Mar 2026	Idaho	Ransomware attack on Kootenai County exposes resident data A ransomware attack detected March 30 hit Kootenai County's network, and the county found criminals took data that may include Social Security, ITIN and driver's license numbers. The county has not said how many residents were affected.	Resident data stolen Coeur d'Alene Press
Mar 2026	New Jersey	Malware attack knocks out Passaic County phones and IT Passaic County said a malware attack took down its phone lines and IT systems used across county government offices. The county said it was working with federal and state officials to investigate and contain the issue.	County of ~600K disrupted The Record

DATE	JURISDICTION	INCIDENT	SCALE · SOURCE
Jan 2026	Connecticut	Cyberattack disrupts New Britain municipal systems A cyberattack detected January 28, 2026, disrupted several New Britain municipal systems and may have exposed names, birth dates, ID numbers, financial and health-related information. The city offered credit monitoring; the number affected was unclear.	Several city systems disrupted Connecticut Public
2026	North Dakota	Ransomware hits Minot water treatment plant server A ransomware attack hit a server at Minot's water treatment plant; the server was unplugged and staff ran manual procedures for about 16 hours. City officials said the water supply remained safe.	16 hours manual operation KFVR-TV
2025			
Dec 2025	Oklahoma	Unauthorized access to taxpayer data in OkTAP portal The Oklahoma Tax Commission identified unauthorized access to tax information in its Oklahoma Taxpayer Access Point (OkTAP) system on Dec. 19, 2025, involving personal and tax information. The state said it is not clear how many individuals were affected.	Number affected unknown Oklahoma OMES (official notice)
Nov 2025	Massachusetts	Attleboro intrusion may have exposed SSNs and medical data Suspicious activity on Attleboro's network ran from October 22 to November 20, 2025, disrupting city systems. In October 2026 the city said exposed data may include Social Security, financial account, driver's license and medical information, and began mailing notices.	Month-long intrusion WJAR (NBC 10)
Sep 2025	Illinois	IDHS maps exposed data on ~700,000 residents for years Internal IDHS resource-planning maps were publicly viewable on a mapping website because of incorrect privacy settings, exposing addresses, case numbers and other details of Medicaid, Medicare Savings Program and rehabilitation services customers. IDHS found the problem on Sept. 22, 2025, restricted access by Sept. 26, and said it knew of no misuse.	About 700,000 residents BleepingComputer
Aug 2025	Nevada	Nevada state offices shut by cyberattack A cyberattack forced Nevada to close state offices and take state websites offline.	Statewide outage ABC News
Aug 2025	Hawaii	Ransomware hits UH Cancer Center, research data of 1.2M exposed Attackers encrypted and stole Epidemiology Division research files, including Social Security numbers, driver's license data and 1998 Honolulu voter registration information. UHCC paid a ransom for a decryptor and data deletion; patient care was not affected.	About 1.24M people HIPAA Journal
Aug 2025	Maryland	Cyberattack disrupts Maryland transit systems, data lost A cyberattack hit the Maryland Transit Administration, disrupting the MobilityLink paratransit reservation system and real-time arrival estimates. MTA confirmed incident-related data loss in September; core bus and MARC services kept running.	Paratransit disrupted The Daily Record
Aug 2025	Pennsylvania	Ransomware takes PA Attorney General's office offline Ransomware encrypted files and took the office's website, email and phone lines offline, and courts granted extensions in some criminal and civil cases. Attorney General Dave Sunday said no ransom was paid.	~1,200 staff, 17 offices Infosecurity Magazine

DATE	JURISDICTION	INCIDENT	SCALE · SOURCE
Aug 2025	Utah	Interlock ransomware steals Box Elder County data, 81,664 notified Box Elder County found ransomware on Aug. 3, 2025, after unauthorized access that began in May. Interlock claimed 4.5 TB of data, and the county refused to pay and notified 81,664 people about exposed data, including Social Security numbers.	81,664 people notified Comparitech
Jul 2025	Arkansas	Cyberattack knocks out Fort Smith schools' phones and internet A cybersecurity incident left all Fort Smith Public School District communication systems, including phone and internet, unavailable, with no restoration timeline as of July 23, 2025. The district brought in a third-party firm for recovery.	Districtwide phones, internet down Talk Business & Politics
Jul 2025	Maine	Cyberattack forces Bar Harbor offline, water plant controls cut After detecting a cyberattack, Bar Harbor physically disconnected municipal systems, including controls that monitor its water and wastewater plants, and closed the town office. The town froze its bank accounts as a precaution and told employees personal data may have been accessed.	Town services offline Bangor Daily News
Jul 2025	Minnesota	Cyberattack on St. Paul prompts National Guard activation A cyberattack beginning July 25 targeted St. Paul's critical systems and digital services and significantly disrupted city services. Gov. Walz activated the Minnesota National Guard's cyber protection forces, citing an attack beyond the city's capacity to respond.	National Guard deployed KTTC
Jun 2025	Arizona	Attackers breach Arizona election candidate portal, post Khomeini image An attacker uploaded code through the Secretary of State's candidate portal and replaced candidate photos on 2016-2024 election results pages with an image of Ayatollah Khomeini. Officials said with moderate confidence that Iran or its affiliates were responsible and that no voter data was accessed; the portal is separate from voter registration and results systems.	Candidate portal shut down Votebeat
May 2025	Alabama	State IT office investigates breach affecting state systems Alabama's Office of Information Technology reported a significant security breach affecting certain state systems, detected on a Friday evening and disclosed May 12, 2025. Some state employee usernames and passwords were compromised; OIT said it believed no residents' personal information was retrieved.	Employee credentials compromised Government Technology
Feb 2025	Virginia	Cyberattack forces Virginia attorney general's office offline The attorney general's office shut down its computer systems after what it called a sophisticated cyberattack on Feb. 12, 2025, and its website stayed down for days. State police and the FBI are investigating.	Agency systems shut down Insurance Journal (Washington Post)
Jan 2025	Nebraska	Nebraska bank network intrusion American National Bank & Trust reported unauthorized network activity on Jan. 21-22. Files touching 66 Nebraska residents were identified.	66 Nebraskans Nebraska Attorney General
Jan 2025	Vermont	Ransomware locks Addison Northwest schools out of servers A ransomware attack locked staff out of district servers and cut internet service at all three schools and the central office. The FBI is investigating, and how much data was taken is unknown.	3 schools, internet down Addison Independent

2024

DATE	JURISDICTION	INCIDENT	SCALE · SOURCE
Dec 2024	Rhode Island	Brain Cipher breach of RIBridges benefits system exposes 644,000 people Brain Cipher used a stolen Deloitte credential to get into the state's RIBridges benefits system in July 2024 and stayed about five months before the state was notified in December 2024. Personal data of an estimated 644,401 applicants and recipients was compromised, and Deloitte has paid the state \$12 million in total.	644,401 people Rhode Island Current
Nov 2024	Michigan ELECTION	Ransomware gang hits Michigan county on Election Day Wexford County's website was compromised on Election Day 2024, and the Embargo ransomware group claimed it stole 1 TB of data. County officials said election security and integrity were not affected and that staff stopped the encryption of county systems.	Claimed 1 TB stolen Comparitech
Oct 2024	Colorado ELECTION	Voting equipment BIOS passwords left exposed on state website BIOS passwords for ballot tabulation equipment sat in a hidden spreadsheet tab on the Secretary of State's website from June until October 24, 2024. Officials called it accidental and said it posed no security threat given physical access controls; staff reset passwords in affected counties.	32 of 64 counties Colorado Public Radio
Oct 2024	Michigan	Cyberattack takes Michigan's largest county offline A cyberattack, reported as ransomware, took all Wayne County government websites offline and disrupted inmate processing, online tax collection and the Register of Deeds. The county investigated with the FBI and Michigan State Police.	All county sites down The Record
Oct 2024	Wisconsin	Chort ransomware steals data on 67,000 Sheboygan residents Hackers breached Sheboygan's systems on Oct. 31, 2024, and the Chort gang claimed the attack. About 67,000 people were affected, with exposed Social Security numbers, state IDs and license plate numbers.	~67,000 people The Record
Oct 2024	Georgia ELECTION	State repels attempt to crash absentee ballot request portal Around Oct. 14, 2024, the Secretary of State's cybersecurity team stopped what officials called a coordinated attempt to crash the absentee ballot portal. Officials did not know who was behind it but said it may have been a foreign nation.	420,000+ simultaneous access attempts Atlanta News First
Sep 2024	Delaware	Ransomware disrupts Delaware public libraries statewide A ransomware attack on a Delaware Libraries server knocked out internet, computer and some phone services at libraries across the state's 35-site system. A RansomHub affiliate claimed stolen data; officials rebuilt systems rather than pay, and said the patron catalog was not affected.	35-site system disrupted The Register
Sep 2024	Rhode Island	Medusa ransomware hits Providence schools, demands \$1M Medusa claimed the attack after the district reported irregular network activity. Internet-connected systems were shut down across the district, and the group demanded \$1 million and threatened to release more than 200 GB of data.	\$1M demand, 200+ GB Rhode Island Current
Aug 2024	Washington	Rhysida ransomware disrupts Sea-Tac and exposes 90,000 people The Port of Seattle blamed Rhysida for an Aug. 24, 2024 attack that disrupted systems at Seattle-Tacoma International Airport. The Port refused a \$6 million ransom and notified about 90,000 people.	90,000 people SecurityWeek

DATE	JURISDICTION	INCIDENT	SCALE · SOURCE
Jul 2024	Florida	RansomHub leaks data stolen from Florida health department A cyberattack on the Florida Department of Health disrupted its vital statistics system for birth and death certificates. RansomHub claimed 100 GB of stolen data and began leaking it after the state refused to pay.	100 GB claimed stolen GovInfoSecurity
Jul 2024	Indiana	Ransomware closes Clay County courthouse; disaster declared A ransomware attack discovered July 9 cut Clay County off from its data and some state partners, closing the courthouse and Health Department and forcing court cases to be rescheduled. The county filed a local disaster declaration; 911 was not affected.	Courthouse closed The Record
Jul 2024	Kentucky	Ransomware shuts Jefferson County Clerk's offices for a week A ransomware attack shut down the Louisville-area clerk's office from July 22 to July 29, closing motor vehicle branches. RansomHub later claimed the attack and said it stole election, motor vehicle and property data; the office had said no data was compromised and did not confirm the group.	Offices closed ~1 week Comparitech
Jul 2024	Ohio	Rhysida ransomware exposes data of 500,000 Columbus residents A July 2024 ransomware attack led Columbus to take critical systems offline, and the Rhysida group claimed it stole 6.5TB of data and posted 3.1TB. The city notified about 500,000 people whose data, including SSNs and bank details, may have been exposed.	~500K people notified Infosecurity Magazine
May 2024	Kansas	Ransomware attackers steal personal, medical data from Franklin County Franklin County said a ransomware attack on its network led cybercriminals to take data on May 19, 2024, including names, Social Security numbers, driver's license and financial account numbers, and medical and vaccination information. The county brought in a forensics team and federal law enforcement.	Personal, medical data stolen Insurance Journal
Apr 2024	Missouri	Ransomware hits Jackson County on election day A ransomware attack disrupted Jackson County systems on April 2, closing assessment, collection and recorder offices, and the county executive declared a state of emergency. The county said its election boards were not affected and voting continued.	State of emergency KCTV5
Mar 2024	Alabama	DDoS attacks slow Alabama state government websites Denial-of-service attacks hit Alabama state government websites in March 2024; the state said its network, data and infrastructure were not accessed or damaged. In October 2024 a federal grand jury indicted two Sudanese nationals alleged to be behind Anonymous Sudan in connection with the attacks.	State websites slowed Alabama Political Reporter
Mar 2024	New Mexico	Ransomware locks prosecutors out of files statewide Ransomware encrypted files on two main servers of the Administrative Office of the District Attorneys, leaving prosecutors without access to their files and disrupting case management. The state's Judicial Information Division warned judges to scrutinize emails from DA addresses.	All 13 judicial districts Government Technology
Feb 2024	Nebraska	Change Healthcare ransomware reaches 575,000+ Nebraskans The attack on the national claims processor exposed data on about 190 million people. Nebraska's attorney general sued after finding at least 575,000 Nebraskans affected.	575,000+ Nebraskans Nebraska Examiner

DATE	JURISDICTION	INCIDENT	SCALE · SOURCE
Jan 2024	Georgia ELECTION	Fulton County, Ga., systems taken down A cyberattack crippled systems in Georgia's largest county, which also runs elections. Repairs were still under way more than a month later.	Countywide outage SecurityWeek
Jan 2024	New Hampshire ELECTION	AI-generated 'Biden' robocall urges NH voters to skip primary A robocall using an AI-generated voice mimicking President Biden told New Hampshire voters to skip the Jan. 23 primary, and it falsely appeared to come from a former state Democratic chair's phone. The NH Attorney General called it an apparent illegal attempt to disrupt and suppress voting.	Statewide primary targeted Associated Press (via Boston.com)
Jan 2024	West Virginia	Cyberattack disrupts Beckley city computer network Beckley announced a cyberattack on its computer network, and the mayor could not say when systems would be restored. The city was still investigating whether any data was affected.	City network disrupted The Record
2023			
Nov 2023	North Carolina	Cyberattack leaves Bladen County operating at limited capacity Hackers accessed Bladen County data, and the county operated in limited capacity without access to some systems. The NC Joint Cybersecurity Task Force was brought in for forensics; life safety services kept running.	County systems limited The Record
Oct 2023	District of Columbia ELECTION	D.C. voter data stolen through a vendor server Hackers took D.C. Board of Elections voter data from a server run by its website vendor. Officials said the attackers may have had access to the full voter roll.	Full voter roll at risk The Record
Oct 2023	Kansas PRIORITY	Kansas court system hit by foreign cyberattack Officials called it a sophisticated foreign cyberattack. Courts in 104 counties were disrupted for weeks, electronic filing went down, and files and case records were stolen.	104 counties disrupted WIBW
Oct 2023	Nevada	Unauthorized party breaches Clark County schools email system Around Oct. 5, 2023, an unauthorized party got into the district's email environment and accessed limited personal information on a subset of students, parents and employees. The district brought in forensic experts, worked with law enforcement and required students to change their passwords.	Subset of students, staff News 3 Las Vegas (KSNV)
Jun 2023	California	MOVEit breach exposes data of 769,000 CalPERS retirees A CalPERS vendor was breached through the MOVEit file-transfer flaw, exposing retirees' and beneficiaries' names, birth dates and Social Security numbers. Officials attributed the theft to Russian cybercriminals; the report names the ClOp group as behind the MOVEit campaign.	About 769,000 people KPBS (AP)
Jun 2023	Louisiana	MOVEit breach exposes records of nearly every Louisiana driver Hackers breached the OMV's MOVEit file transfer system, exposing names, addresses, license photos, height and weight. The OMV believes everyone with a state license, ID or vehicle registration likely had data exposed.	6M+ records WAFB

DATE	JURISDICTION	INCIDENT	SCALE · SOURCE
Jun 2023	Missouri	MOVEit breach via IBM exposes Missouri Medicaid data Data was stolen through a MOVEit vulnerability in a tool IBM used for DSS, exposing Medicaid participants' names, client numbers, birth dates and claims data. DSS planned to notify all Medicaid participants and providers enrolled in May 2023.	All Medicaid enrollees The Record
Jun 2023	Oregon	MOVEit hack exposes 3.5M Oregon driver's license records Attackers exploited the MOVEit file transfer tool used by ODOT and accessed files with names, license or ID numbers, birth dates, addresses and partial SSNs. The data covers about 3.5 million current Oregon license and ID holders; ClOp claimed the MOVEit attack.	3.5M records Oregon DOT (official notice)
May 2023	Colorado	MOVEit breach exposes data of 4 million Colorado Medicaid members An unauthorized party accessed HCPF files that service provider IBM was transferring with MOVEit, exposing names, Social Security numbers, medical and insurance information of Health First Colorado and CHP+ members. HCPF said its own systems were not impacted.	About 4.1M people SecurityWeek
May 2023	Maine	MOVEit breach hits roughly the entire population of Maine Attackers exploited a zero-day in the state's MOVEit server on May 28-29, stealing files tied to health and human services, education, motor vehicles, corrections, unemployment and other agencies. Maine disclosed in November that about 1.3 million people were affected.	1.3M people Cybersecurity Dive
May 2023	Texas	Royal ransomware shuts Dallas courts, disrupts police systems The city said the Royal group was behind a ransomware attack that significantly affected police operations, including computer-aided dispatch, and closed municipal courts. The 311 site and utility payments also went down, while 911 dispatch stayed operational.	Courts closed, police CAD down Dallas Morning News
Apr 2023	Montana	Cyberattack on MSU brings in Montana National Guard A cyberattack hit Montana State University's Bozeman and Great Falls campuses on April 19. The National Guard's cyber team helped isolate the threat and keep it from spreading.	Two campuses affected NBC Montana
Apr 2023	South Carolina	Ransomware attack disrupts Spartanburg County IT and phone systems A ransomware attack limited Spartanburg County's IT and phone systems. 911 and emergency communications kept running, and the state Judicial Branch said its systems were not affected.	County IT, phones limited The Record
Mar 2023	Tennessee	Ransomware attack takes Oak Ridge city network offline A ransomware attack hit Oak Ridge, a city of about 31,000, taking down its network and website. Police and fire stayed reachable by phone while the city worked with law enforcement and recovery specialists.	City network, website down The Record
Feb 2023	Minnesota	Medusa leaks Minneapolis schools data after \$1M demand The Medusa ransomware group attacked the district, demanded \$1 million, and posted stolen data when it refused to pay. The leak reportedly included student records, health and disciplinary files, addresses, and payroll data.	34,500-student district The Record

DATE	JURISDICTION	INCIDENT	SCALE · SOURCE
Feb 2023	West Virginia	Cyberattack cancels classes for 20,000 Berkeley County students A cyberattack caused internet and phone outages at West Virginia's second-largest school district, and classes were canceled for nearly 20,000 students. The district said it did not know at the time whether personal data was breached.	~20,000 students out The Record
Jan 2023	Iowa PRIORITY	Des Moines Public Schools hit by ransomware Iowa's largest school district took its network offline after a ransomware attack. Personal data of nearly 6,700 people was taken.	~6,700 people District Administration
Jan 2023	Hawaii	Stolen login used to access Hawaii death registry records Credentials for an unused external death certifier account were sold on the dark web and used to access the state's Electronic Death Registry System. Records exposed names, Social Security numbers, addresses and causes of death; the attacker has not been identified.	About 3,400 records The Record
2022			
Dec 2022	Iowa PRIORITY	Hack at records vendor cuts Iowa counties off from land records Cott Systems, an Ohio company that hosts public records for government agencies, appears to have been hacked over the holidays, and the FBI was reportedly investigating. Iowa county recorders, including Dallas County, lost access to real estate records, and the system had not been fully restored by early January 2023.	300+ agencies, 21 states Iowa Capital Dispatch
Nov 2022	Arkansas	Vendor cyberattack takes Arkansas county offices offline A cyberattack on Apprentice Information Systems, which stores data for county tax collector, assessor, clerk and treasurer offices, led many Arkansas counties to take systems offline. Boone County's collector issued handwritten receipts while systems were down.	Many county offices offline KY3
Nov 2022	Mississippi ELECTION	Election Day DDoS knocks Secretary of State sites offline On Election Day, a DDoS attack intermittently made public-facing Secretary of State websites unavailable. The office said the election system was not compromised and did not attribute the attack.	Intermittent outage Mississippi Secretary of State
Oct 2022	Kentucky ELECTION	Pro-Russian DDoS knocks Kentucky elections and courts sites offline A denial-of-service attack took down several Kentucky state sites, including the Board of Elections page, the Department of Education site and state court websites. The pro-Kremlin group Killnet claimed responsibility; the state's vendor said there was no evidence data was compromised.	Sites down ~1 day Louisville Public Media
Sep 2022	New York	BlackCat ransomware cripples Suffolk County government Attackers entered through the county clerk's office via Log4j in December 2021 and deployed ransomware in September 2022, disabling email for over 10,000 workers and forcing dispatchers to take calls by hand for weeks. About 400GB of stolen data was leaked; the BlackCat/AlphV group claimed the attack and the county did not pay.	~\$5.5M cost; 400GB leaked The Record
May 2022	New Jersey ELECTION	Ransomware hits Somerset County weeks before NJ primary Ransomware disabled Somerset County's email server and other services, which affected the county clerk's office and could slow mail-in ballot requests before the June 7 primary. Officials said the systems used to cast, process and count ballots were not affected.	County email, services down StateScoop

DATE	JURISDICTION	INCIDENT	SCALE · SOURCE
Jan 2022	New Mexico ELECTION	Ransomware halts Bernalillo County voter registration, jail locks A ransomware attack discovered Jan. 5 took county systems offline, and the clerk's office could not register voters, issue marriage licenses or approve deed transfers. At the Metropolitan Detention Center, electronic cell locks and cameras failed and the jail was locked down.	Countywide; weeks of disruption TechTarget
2021			
Dec 2021	Virginia	Ransomware hits Virginia legislature's IT agency, websites A ransomware attack hit the Division of Legislative Automated Systems and spread to nearly all legislative websites. The director said most of the state's critical systems were locked, and a ransom note was received.	Legislative IT shut down UPI
Aug 2021	New Hampshire	Email fraud diverts \$2.3M in Peterborough town funds Thieves posing as school district staff used forged documents and email accounts to redirect two town payments, one meant for the school district and one for bridge contractors. The town canceled all ACH transfers, and the U.S. Secret Service investigated.	\$2.3M stolen New Hampshire Public Radio
Jun 2021	Massachusetts	Ransomware hits state ferry agency, delaying ticketing A ransomware attack starting June 2 hit the state agency that runs ferries to Martha's Vineyard and Nantucket, taking its website offline and delaying ticketing. Ferries kept running; the agency said no sensitive data was accessed and no ransom was paid.	Ticketing down ~2 weeks SecurityWeek
May 2021	Alaska	Nation-state attackers breach Alaska health department network Attackers the department described as a nation-state sponsored group entered DHSS's internal network through a website vulnerability. Breached systems stayed offline for months, forcing manual processing of background checks and vital records, and any data on the agency's systems may have been exposed.	Systems offline for months The Record
May 2021	Oklahoma	Tulsa ransomware shuts city services, leaks 18,000 files Ransomware hit Tulsa's online bill payment, utility billing, email, websites, police and 311 systems, and the city shut down all services to stop the spread. After the city refused to pay, attackers leaked more than 18,000 files, mostly police citations and employee files.	18,000+ files leaked Route Fifty
Apr 2021	Wyoming PRIORITY	Wyoming health test data posted to public GitHub A Wyoming Department of Health employee uploaded files to GitHub that held lab test results for 164,021 people, about one in four state residents.	164,021 people Wyoming Department of Health
Feb 2021	Washington	Accellion breach may expose 1.6M Washington jobless claims Attackers compromised Accellion file-transfer software used by the State Auditor. Names, Social Security numbers and bank information of about 1.6 million people who filed for unemployment in 2020 may have been exposed.	1.6M claimants Northwest Public Broadcasting
2020			
Nov 2020	Pennsylvania	Ransomware encrypts Delaware County police and payroll data Attackers took control of Delaware County's government network and encrypted files including police reports, payroll and purchasing records. They demanded \$500,000, which sources said the county was in the process of paying through insurance.	\$500K ransom demand 6abc Philadelphia

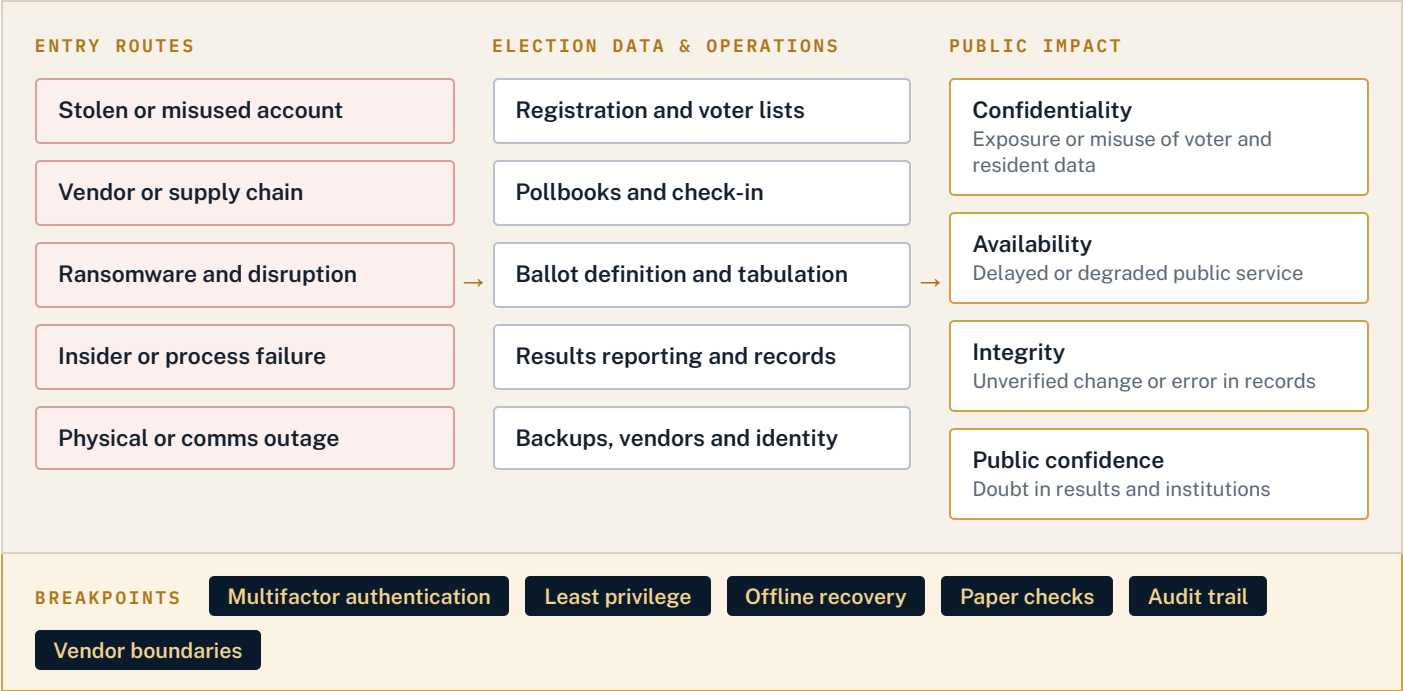
DATE	JURISDICTION	INCIDENT	SCALE · SOURCE
Oct 2020	Alaska ELECTION	Hackers steal Alaska voter data from online registration system Outside actors gained unauthorized access to data in Alaska's online voter registration system, exposing names, birth dates, driver's license numbers, addresses, party affiliations and partial Social Security numbers. Officials said the breach did not affect election results and that no other election systems were affected.	100,000+ voters Alaska Public Media
Oct 2020	New York ELECTION	Ransomware days before election puts absentee requests at risk A cyberattack encrypted about 200 Chenango County computers, raising concern that emailed absentee ballot applications might not be processed. The county board told voters who emailed applications after Oct. 15 to call and confirm receipt; the state said overall voting would not be affected.	~200 computers encrypted WSKG
Jul 2020	Utah	University of Utah pays \$457,000 after ransomware attack Attackers encrypted servers in the university's College of Social and Behavioral Science and stole student and employee data first. The university's cyber insurer paid \$457,059 to stop the data from being released.	\$457K ransom paid BleepingComputer
Apr 2020	North Dakota	Maze ransomware hits fiber provider for ND state network Ransomware hit Dakota Carrier Network, which operates fiber supporting STAGEnet, the statewide network shared by state government and about 400 public entities. Administrative files were posted online by the Maze group; DCN reported no disruption to fiber service.	Admin files leaked StateScoop
2019			
Nov 2019	Louisiana	Attempted ransomware attack disrupts nearly every state agency An attempted ransomware attack led the state's Office of Technology Services to take its servers offline, shutting down many state websites and email systems. Officials said nearly every state agency was affected, and full restoration was expected to take several days.	Nearly all agencies hit Insurance Journal (AP)
Nov 2019	Ohio ELECTION	Attackers try to inject code into Ohio SOS website The Ohio Secretary of State's office was targeted by an attempt to insert code into its website, originating from a computer in Panama. A spokesperson said data was not at risk.	Attempt blocked; no data lost WCBE
Aug 2019	Texas	Coordinated ransomware attack hits 23 Texas local governments The Texas Department of Information Resources said 23 mostly small local governments were hit by ransomware that came from a single threat actor. The state activated an emergency response, and state systems were not affected.	23 local governments KERA News
May 2019	Maryland	RobbinHood ransomware cripples Baltimore city network A ransomware attack using the RobbinHood variant hobbled Baltimore's computer network; attackers demanded about \$76,000 in bitcoin and the city refused to pay. The budget office estimated the cost at at least \$18.2 million.	\$18.2M cost NBC Washington (AP)
Jan 2019	Oregon	Phishing exposes data of 645,000 Oregon DHS clients Nine DHS employees fell for a phishing email, giving an attacker access to mailboxes holding up to two million emails for about 20 days. Exposed data included names, SSNs, birth dates and protected health information.	645,000 people BleepingComputer

DATE	JURISDICTION	INCIDENT	SCALE · SOURCE
2018			
May 2018	Idaho	Hackers deface Idaho Legislature and iCourt websites On May 11, 2018, the Idaho Legislative Services Office and iCourt web pages were defaced and taken down to add security measures. A group called AnonPlus claimed it; the state said no sensitive information was compromised.	2 sites taken down KIVI-TV
May 2018	Tennessee ELECTION	Election-night results website knocked offline in Knox County Knox County's election results website went down for about an hour after polls closed in the May 1 primary. A security firm linked the crash to a likely denial-of-service attack plus suspicious foreign access, and officials said no voting data was affected.	Results site down ~1 hour Phys.org (AP)
2017			
Dec 2017	North Carolina	LockCrypt ransomware hits Mecklenburg County; ransom refused After an employee opened an email attachment, LockCrypt ransomware encrypted 48 of the county's 500 servers, disrupting courts, tax, register of deeds, health and human services and other offices. The county refused a \$23,000 ransom demand and rebuilt from backups.	48 servers encrypted NACo County News
Sep 2017	Montana	School network hack closes 30+ Flathead Valley schools A hacker breached the Columbia Falls district's system and used the data to send threats to students and families to extort money. More than 30 schools canceled classes; authorities named The Dark Overlord.	15,000+ students home CBS News
Sep 2017	Wisconsin ELECTION	DHS confirms Russian hackers targeted Wisconsin in 2016 DHS told Wisconsin that Russian hackers scanned state computer systems in 2016 and tried to place an ad linking to a suspicious IP address on a state computer. The Elections Commission said no systems were hacked and no voter records or votes were changed.	Attempts, no breach WPR
Mar 2017	Vermont	Joblink breach puts unemployment filers' SSNs at risk A breach of Joblink, the job-search database Vermont unemployment filers must use, may have exposed Social Security numbers. The vendor, America's Job Link Alliance, said more than 180,000 accounts were compromised, including tens of thousands of Vermonters.	180,000+ accounts Vermont Public
2016			
Nov 2016	Indiana ELECTION	Ransomware halts online posting of county election results A ransomware attack disabled the server Madison County used to post election results online, so the clerk's office tallied by hand and handed out printed results. Officials said votes cast were not affected; the county paid the ransom on its insurer's advice.	Results site offline Meridian Star (AP)
Nov 2016	South Carolina ELECTION	Nearly 150,000 attempts to penetrate S.C. voter registration system South Carolina's voter registration system saw nearly 150,000 attempts to penetrate it on Election Day 2016. A later DHS scan requested by the state found 55 vulnerabilities on four State Election Commission devices.	~150,000 attempts GovTech (via The State)

DATE	JURISDICTION	INCIDENT	SCALE · SOURCE
Jun 2016	Illinois ELECTION	Illinois voter registration database breached Russian military intelligence officers accessed the Illinois State Board of Elections voter registration database, according to the Senate Intelligence Committee. State officials notified affected voters.	Statewide voter rolls CBS Chicago
Jun 2016	California ELECTION	Riverside DA: hackers altered voters' party registrations in 2016 The Riverside County District Attorney said hackers accessed the state's online voter registration system and changed some voters' party affiliations, causing confusion at the June 2016 primary. The perpetrators are unknown, and the Secretary of State's office said it had no evidence of a breach of its database.	20 formal voter complaints KQED
2016	Arizona ELECTION	Malware attempt via Gila County targets Arizona voter database A Gila County elections worker opened a malicious email attachment in an attempt aimed at servers holding about 4 million voters' records; the FBI alerted the Secretary of State, who said the voter database was not breached. Experts cited in the report believed the Russian government was responsible.	4M voter records targeted CBS News
2016	Connecticut ELECTION	Russian agents targeted Connecticut voter registration system DHS notified Connecticut that its online voter registration database was one of 21 states' systems targeted by Russian agents before the 2016 election. The Secretary of the State said the state's intrusion detection system stopped the attempt.	Attempt blocked Connecticut Secretary of the State
2016	Delaware ELECTION	Russian hackers attempted to access Delaware voter registration DHS told Delaware it was among 21 states hit by attempts to access voter data before the 2016 election. The state elections commissioner said the attempts on the voter registration system were unsuccessful.	Attempt unsuccessful Delaware Public Media
2016	Florida ELECTION	Russian-linked hackers accessed voter data in two Florida counties Gov. Ron DeSantis said in 2019 that Russia-affiliated actors accessed voter databases in two counties in 2016 via phishing emails posing as vendor VR Systems. He said the data was publicly available and the breach did not affect votes or results; the counties were not named.	2 county voter databases WFSU

Route to harm, and where to break it

How an intrusion travels from entry point to public impact, mapped to the CISA and EAC election-security framework, with the controls that stop it.



THREAT PATHWAY	CONSEQUENCE	EVIDENCE TO REQUEST OR TEST	RESILIENCE RESPONSE
Compromised identity	Unauthorized access or record changes	Role list, MFA coverage, privileged-access logs, revocation timing	Least privilege, independent approval, monitored account lifecycle
Vendor dependency	Service interruption or data exposure	System inventory, contract controls, subcontractors, incident terms	Bounded vendor access, continuity plan, exit and recovery procedure
Ransomware	Delay, degraded service, loss of access	Offline backup evidence, restoration results, outage procedures	Offline recovery, paper fallback, timed recovery exercises
Insider or process error	Unreviewed action or custody gap	Separation of duties, custody logs, exception records	Dual control, tamper-evident seals, independent reconciliation
False information	Voter confusion, reduced confidence	Communication roles, correction speed, official-source links	Pre-approved response path, accessible public updates

Every state, on one page

2025 FBI cybercrime figures and the documented public-sector incidents in each jurisdiction, alphabetical.

Alabama AL • South

#46 of 51

9,936	191	\$167.2M	\$32
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

May 2025 State IT office investigates breach affecting state systems. Government Technology

Mar 2024 DDoS attacks slow Alabama state government websites. Alabama Political Reporter

California CA • West

#13 of 51

116,414	296	\$3.6B	\$93
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jun 2023 MOVEit breach exposes data of 769,000 CalPERS retirees. KPBS (AP)

Jun 2016 Riverside DA: hackers altered voters' party registrations in 2016. KQED

Alaska AK • West

#2 of 51

3,202	434	\$40.0M	\$54
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

May 2021 Nation-state attackers breach Alaska health department network. The Record

Oct 2020 Hackers steal Alaska voter data from online registration system. Alaska Public Media

Colorado CO • West

#7 of 51

18,847	314	\$355.0M	\$59
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Oct 2024 Voting equipment BIOS passwords left exposed on state website. Colorado Public Radio

May 2023 MOVEit breach exposes data of 4 million Colorado Medicaid members. SecurityWeek

Arizona AZ • West

#4 of 51

28,868	379	\$630.7M	\$83
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jun 2025 Attackers breach Arizona election candidate portal, post Khomeini image. Votebeat

2016 Malware attempt via Gila County targets Arizona voter database. CBS News

Connecticut CT • Northeast

#25 of 51

9,714	263	\$219.5M	\$60
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jan 2026 Cyberattack disrupts New Britain municipal systems. Connecticut Public

2016 Russian agents targeted Connecticut voter registration system. Connecticut Secretary of the State

Arkansas AR • South

#45 of 51

6,161	198	\$102.5M	\$33
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jul 2025 Cyberattack knocks out Fort Smith schools' phones and internet. Talk Business & Politics

Nov 2022 Vendor cyberattack takes Arkansas county offices offline. KY3

Delaware DE • South

#15 of 51

3,089	291	\$62.0M	\$59
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Sep 2024 Ransomware disrupts Delaware public libraries statewide. The Register

2016 Russian hackers attempted to access Delaware voter registration. Delaware Public Media

District of Columbia DC · South #1 of 51

3,113	449	\$97.4M	\$140
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jun 2026 Cyberattack compromises D.C. Housing Authority systems, website down. WJLA 7News

Oct 2023 D.C. voter data stolen through a vendor server. The Record

Illinois IL · Midwest #26 of 51

32,977	259	\$535.3M	\$42
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Sep 2025 IDHS maps exposed data on ~700,000 residents for years. BleepingComputer

Jun 2016 Illinois voter registration database breached. CBS Chicago

Florida FL · South #11 of 51

71,843	306	\$1.6B	\$68
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jul 2024 RansomHub leaks data stolen from Florida health department. GovInfoSecurity

2016 Russian-linked hackers accessed voter data in two Florida counties. WFSU

Indiana IN · Midwest #12 of 51

20,777	298	\$233.0M	\$33
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jul 2024 Ransomware closes Clay County courthouse; disaster declared. The Record

Nov 2016 Ransomware halts online posting of county election results. Meridian Star (AP)

Georgia GA · South #35 of 51

25,936	230	\$534.6M	\$47
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Oct 2024 State repels attempt to crash absentee ballot request portal. Atlanta News First

Jan 2024 Fulton County, Ga., systems taken down. SecurityWeek

Iowa IA · Midwest · Priority #51 of 51

5,436	168	\$95.5M	\$30
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jan 2023 Des Moines Public Schools hit by ransomware. District Administration

Dec 2022 Hack at records vendor cuts Iowa counties off from land records. Iowa Capital Dispatch

Hawaii HI · West #32 of 51

3,328	232	\$106.4M	\$74
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Aug 2025 Ransomware hits UH Cancer Center, research data of 1.2M exposed. HIPAA Journal

Jan 2023 Stolen login used to access Hawaii death registry records. The Record

Kansas KS · Midwest · Priority #22 of 51

7,927	266	\$147.3M	\$49
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

May 2024 Ransomware attackers steal personal, medical data from Franklin County. Insurance Journal

Oct 2023 Kansas court system hit by foreign cyberattack. WIBW

Idaho ID · West #40 of 51

4,479	221	\$88.7M	\$44
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Mar 2026 Ransomware attack on Kootenai County exposes resident data. Coeur d'Alene Press

May 2018 Hackers deface Idaho Legislature and iCourt websites. KIVI-TV

Kentucky KY · South #43 of 51

9,414	204	\$119.7M	\$26
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jul 2024 Ransomware shuts Jefferson County Clerk's offices for a week. Comparitech

Oct 2022 Pro-Russian DDoS knocks Kentucky elections and courts sites offline. Louisville Public Media

Louisiana LA • South

#47 of 51

8,623	187	\$105.4M	\$23
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jun 2023 MOVEit breach exposes records of nearly every Louisiana driver. WAFB

Nov 2019 Attempted ransomware attack disrupts nearly every state agency. Insurance Journal (AP)

Minnesota MN • Midwest

#31 of 51

13,595	233	\$248.9M	\$43
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jul 2025 Cyberattack on St. Paul prompts National Guard activation. KTTC

Feb 2023 Medusa leaks Minneapolis schools data after \$1M demand. The Record

Maine ME • Northeast

#44 of 51

2,888	204	\$56.5M	\$40
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jul 2025 Cyberattack forces Bar Harbor offline, water plant controls cut. Bangor Daily News

May 2023 MOVEit breach hits roughly the entire population of Maine. Cybersecurity Dive

Mississippi MS • South

#50 of 51

5,084	172	\$77.4M	\$26
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Oct 2026 Ransomware forces Vicksburg to shut down city systems. The Record

Nov 2022 Election Day DDoS knocks Secretary of State sites offline. Mississippi Secretary of State

Maryland MD • South

#8 of 51

19,430	310	\$390.2M	\$62
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Aug 2025 Cyberattack disrupts Maryland transit systems, data lost. The Daily Record

May 2019 RobbinHood ransomware cripples Baltimore city network. NBC Washington (AP)

Missouri MO • Midwest

#38 of 51

14,087	225	\$233.9M	\$37
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Apr 2024 Ransomware hits Jackson County on election day. KCTV5

Jun 2023 MOVEit breach via IBM exposes Missouri Medicaid data. The Record

Massachusetts MA • Northeast

#5 of 51

22,936	321	\$410.9M	\$57
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Nov 2025 Attleboro intrusion may have exposed SSNs and medical data. WJAR (NBC 10)

Jun 2021 Ransomware hits state ferry agency, delaying ticketing. SecurityWeek

Montana MT • West

#36 of 51

2,618	229	\$53.2M	\$46
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Apr 2023 Cyberattack on MSU brings in Montana National Guard. NBC Montana

Sep 2017 School network hack closes 30+ Flathead Valley schools. CBS News

Michigan MI • Midwest

#41 of 51

22,191	219	\$381.1M	\$38
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Nov 2024 Ransomware gang hits Michigan county on Election Day. Comparitech

Oct 2024 Cyberattack takes Michigan's largest county offline. The Record

Nebraska NE • Midwest • Priority

#48 of 51

3,724	185	\$71.8M	\$36
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jan 2025 Nebraska bank network intrusion. Nebraska Attorney General

Feb 2024 Change Healthcare ransomware reaches 575,000+ Nebraskans. Nebraska Examiner

Nevada NV · West

#3 of 51

13,366	407	\$302.2M	\$92
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

- Aug 2025 Nevada state offices shut by cyberattack. ABC News
- Oct 2023 Unauthorized party breaches Clark County schools email system. News 3 Las Vegas (KSNV)

North Carolina NC · South

#34 of 51

25,940	232	\$431.6M	\$39
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

- Nov 2023 Cyberattack leaves Bladen County operating at limited capacity. The Record
- Dec 2017 LockCrypt ransomware hits Mecklenburg County; ransom refused. NACo County News

New Hampshire NH · Northeast

#9 of 51

4,374	309	\$59.3M	\$42
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

- Jan 2024 AI-generated 'Biden' robocall urges NH voters to skip primary. Associated Press (via Boston.com)
- Aug 2021 Email fraud diverts \$2.3M in Peterborough town funds. New Hampshire Public Radio

North Dakota ND · Midwest

#49 of 51

1,418	177	\$37.9M	\$47
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

- 2026 Ransomware hits Minot water treatment plant server. KFYY-TV
- Apr 2020 Maze ransomware hits fiber provider for ND state network. StateScoop

New Jersey NJ · Northeast

#42 of 51

20,648	216	\$660.4M	\$69
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

- Mar 2026 Malware attack knocks out Passaic County phones and IT. The Record
- May 2022 Ransomware hits Somerset County weeks before NJ primary. StateScoop

Ohio OH · Midwest

#33 of 51

27,626	232	\$421.3M	\$35
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

- Jul 2024 Rhysida ransomware exposes data of 500,000 Columbus residents. Infosecurity Magazine
- Nov 2019 Attackers try to inject code into Ohio SOS website. WCBE

New Mexico NM · West

#21 of 51

5,688	268	\$85.6M	\$40
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

- Mar 2024 Ransomware locks prosecutors out of files statewide. Government Technology
- Jan 2022 Ransomware halts Bernalillo County voter registration, jail locks. TechTarget

Oklahoma OK · South

#16 of 51

11,964	290	\$131.9M	\$32
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

- Dec 2025 Unauthorized access to taxpayer data in OkTAP portal. Oklahoma OMES (official notice)
- May 2021 Tulsa ransomware shuts city services, leaks 18,000 files. Route Fifty

New York NY · Northeast

#37 of 51

45,255	226	\$1.2B	\$61
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

- Sep 2022 BlackCat ransomware cripples Suffolk County government. The Record
- Oct 2020 Ransomware days before election puts absentee requests at risk. WSKG

Oregon OR · West

#14 of 51

12,477	292	\$193.2M	\$45
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

- Jun 2023 MOVEit hack exposes 3.5M Oregon driver's license records. Oregon DOT (official notice)
- Jan 2019 Phishing exposes data of 645,000 Oregon DHS clients. BleepingComputer

Pennsylvania PA · Northeast

#29 of 51

31,154	239	\$537.8M	\$41
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Aug 2025 Ransomware takes PA Attorney General's office offline. Infosecurity Magazine

Nov 2020 Ransomware encrypts Delaware County police and payroll data. 6abc Philadelphia

Texas TX · South

#10 of 51

97,912	309	\$1.8B	\$58
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

May 2023 Royal ransomware shuts Dallas courts, disrupts police systems. Dallas Morning News

Aug 2019 Coordinated ransomware attack hits 23 Texas local governments. KERA News

Rhode Island RI · Northeast

#28 of 51

2,700	242	\$72.0M	\$65
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Dec 2024 Brain Cipher breach of RIBridges benefits system exposes 644,000 people. Rhode Island Current

Sep 2024 Medusa ransomware hits Providence schools, demands \$1M. Rhode Island Current

Utah UT · West

#18 of 51

9,903	280	\$195.4M	\$55
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Aug 2025 Interlock ransomware steals Box Elder County data, 81,664 notified. Comparitech

Jul 2020 University of Utah pays \$457,000 after ransomware attack. BleepingComputer

South Carolina SC · South

#23 of 51

14,699	264	\$264.1M	\$47
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Apr 2023 Ransomware attack disrupts Spartanburg County IT and phone systems. The Record

Nov 2016 Nearly 150,000 attempts to penetrate S.C. voter registration system. GovTech (via The State)

Vermont VT · Northeast

#27 of 51

1,580	245	\$26.6M	\$41
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Jan 2025 Ransomware locks Addison Northwest schools out of servers. Addison Independent

Mar 2017 Joblink breach puts unemployment filers' SSNs at risk. Vermont Public

South Dakota SD · Midwest

#20 of 51

Priority

2,514	269	\$51.5M	\$55
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Aug 2026 Cyberattack hits part of Mitchell city computer network. Dakota News Now

Jul 2026 Pennington County, S.D., systems knocked out. South Dakota Searchlight

Virginia VA · South

#17 of 51

25,314	285	\$476.1M	\$54
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Feb 2025 Cyberattack forces Virginia attorney general's office offline. Insurance Journal (Washington Post)

Dec 2021 Ransomware hits Virginia legislature's IT agency, websites. UPI

Tennessee TN · South

#39 of 51

16,261	222	\$269.2M	\$37
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Mar 2023 Ransomware attack takes Oak Ridge city network offline. The Record

May 2018 Election-night results website knocked offline in Knox County. Phys.org (AP)

Washington WA · West

#6 of 51

25,619	320	\$458.2M	\$57
COMPLAINTS	PER 100K	LOSSES	PER RESIDENT

Aug 2024 Rhysida ransomware disrupts Sea-Tac and exposes 90,000 people. SecurityWeek

Feb 2021 Accellion breach may expose 1.6M Washington jobless claims. Northwest Public Broadcasting

West Virginia WV · South

#30 of 51

4,209

COMPLAINTS

238

PER 100K

\$92.6M

LOSSES

\$52

PER RESIDENT

Jan 2024 Cyberattack disrupts Beckley city computer network. *The Record*

Feb 2023 Cyberattack cancels classes for 20,000 Berkeley County students. *The Record*

Wyoming WY · West · Priority

#24 of 51

1,552

COMPLAINTS

264

PER 100K

\$25.8M

LOSSES

\$44

PER RESIDENT

Sep 2026 Court vendor breach exposes Wyoming court users' personal data. *Wyoming Public Media*

Apr 2021 Wyoming health test data posted to public GitHub. *Wyoming Department of Health*

Wisconsin WI · Midwest

#19 of 51

16,680

COMPLAINTS

279

PER 100K

\$194.2M

LOSSES

\$33

PER RESIDENT

Oct 2024 Chort ransomware steals data on 67,000 Sheboygan residents. *The Record*

Sep 2017 DHS confirms Russian hackers targeted Wisconsin in 2016. *WPR*

Show the risk, then the response

Ten frames for presentations, each built around one part of the resilience story.



01 • Data pathway

Entry routes meet protective checkpoints before reaching public records.



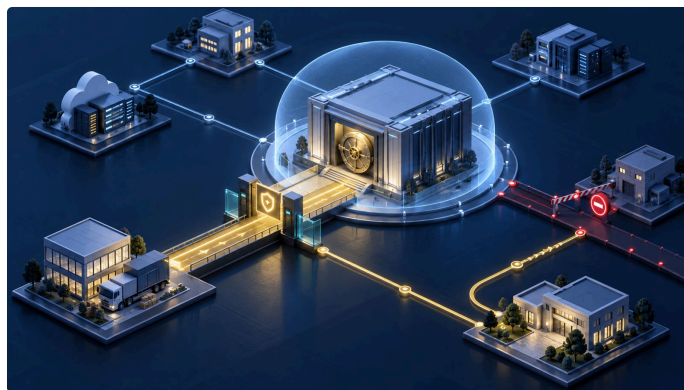
02 • Service continuity

A degraded digital service beside a working paper continuity path.



03 • Account access

Misused credentials stopped; authorized access passes.



04 • Vendor boundaries

A monitored vendor route and an available alternate path.



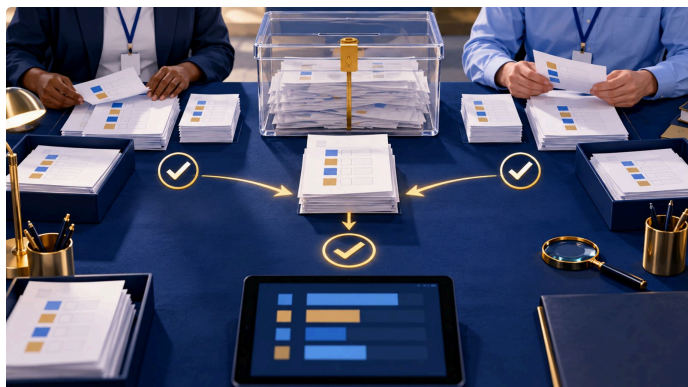
05 • Chain of custody

Independent handling and sealed evidence make review possible.



06 • Physical continuity

Paper procedures and backup radios keep a local office running.



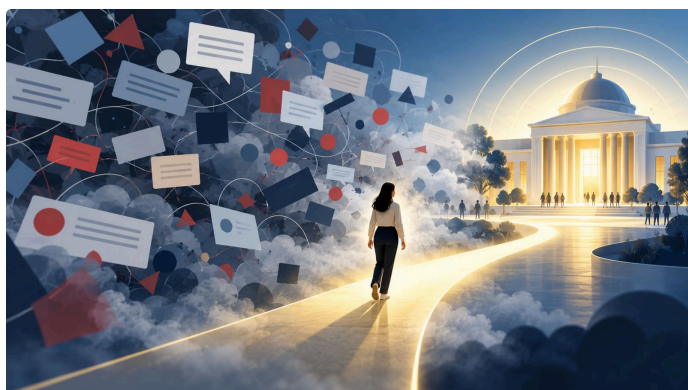
07 • Integrity checks

Bipartisan paper-based checks support reconciliation.



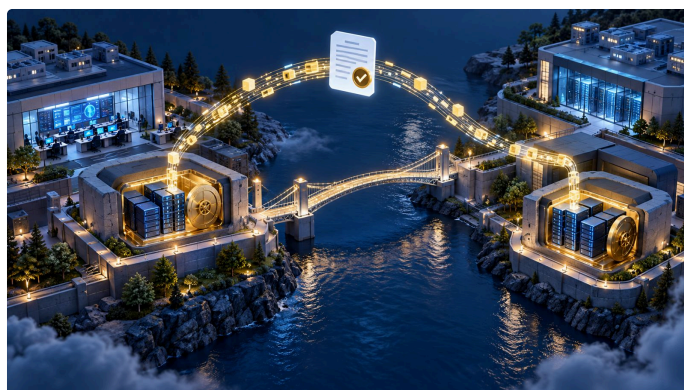
08 • Data privacy

Sensitive records stay sealed; only a minimal exchange moves.



09 • Public information

Clear official communication cuts through noise.



10 • Recovery architecture

Separated backup sites linked by a tested recovery bridge.

From baseline to proven recovery

A phased readiness program that starts in the priority region and scales to every jurisdiction that opts in.

PHASE 1

Establish the baseline

- Confirm the system boundary, data owners and decision-makers.
- Inventory data flows, vendors, user roles, backups and paper dependencies.
- Agree on privacy rules, evidence custody and evaluation criteria.

PHASE 2

Test recovery and proof

- Run tabletop and recovery exercises in an isolated environment.
- Measure restoration time, evidence completeness, access revocation and reconciliation.
- Deliver findings with corrective actions and independent review.

PHASE 3

Scale state by state

- Carry the tested playbook from the priority region to additional states.
- Track each jurisdiction against the same recovery and custody measures.
- Publish a recurring national resilience scorecard.



Decision requested

Authorize a scoping session to set the evidence, owners, safeguards and success measures for a readiness assessment.

SOURCES

Trace every figure

1. FBI Internet Crime Complaint Center, 2025 IC3 Annual Report
2. U.S. Census Bureau, Vintage 2025 state population estimates
3. CISA, Election Security
4. U.S. Election Assistance Commission, Election Security Preparedness
5. **AL** Alabama Political Reporter, "DDoS attacks slow Alabama state government websites" (Mar 2024)
6. **AL** Government Technology, "State IT office investigates breach affecting state systems" (May 2025)
7. **AK** Alaska Public Media, "Hackers steal Alaska voter data from online registration system" (Oct 2020)
8. **AK** The Record, "Nation-state attackers breach Alaska health department network" (May 2021)
9. **AZ** CBS News, "Malware attempt via Gila County targets Arizona voter database" (2016)
10. **AZ** Votebeat, "Attackers breach Arizona election candidate portal, post Khomeini image" (Jun 2025)
11. **AR** KY3, "Vendor cyberattack takes Arkansas county offices offline" (Nov 2022)
12. **AR** Talk Business & Politics, "Cyberattack knocks out Fort Smith schools' phones and internet" (Jul 2025)
13. **CA** KQED, "Riverside DA: hackers altered voters' party registrations in 2016" (Jun 2016)
14. **CA** KPBS (AP), "MOVEit breach exposes data of 769,000 CalPERS retirees" (Jun 2023)
15. **CO** SecurityWeek, "MOVEit breach exposes data of 4 million Colorado Medicaid members" (May 2023)
16. **CO** Colorado Public Radio, "Voting equipment BIOS passwords left exposed on state website" (Oct 2024)
17. **CT** Connecticut Secretary of the State, "Russian agents targeted Connecticut voter registration system" (2016)
18. **CT** Connecticut Public, "Cyberattack disrupts New Britain municipal systems" (Jan 2026)
19. **DE** Delaware Public Media, "Russian hackers attempted to access Delaware voter registration" (2016)
20. **DE** The Register, "Ransomware disrupts Delaware public libraries statewide" (Sep 2024)
21. **DC** The Record, "D.C. voter data stolen through a vendor server" (Oct 2023)
22. **DC** WJLA 7News, "Cyberattack compromises D.C. Housing Authority systems, website down" (Jun 2026)

23. **FL** WFSU, "Russian-linked hackers accessed voter data in two Florida counties" (2016)
24. **FL** GovInfoSecurity, "RansomHub leaks data stolen from Florida health department" (Jul 2024)
25. **GA** SecurityWeek, "Fulton County, Ga., systems taken down" (Jan 2024)
26. **GA** Atlanta News First, "State repels attempt to crash absentee ballot request portal" (Oct 2024)
27. **HI** The Record, "Stolen login used to access Hawaii death registry records" (Jan 2023)
28. **HI** HIPAA Journal, "Ransomware hits UH Cancer Center, research data of 1.2M exposed" (Aug 2025)
29. **ID** KIVI-TV, "Hackers deface Idaho Legislature and iCourt websites" (May 2018)
30. **ID** Coeur d'Alene Press, "Ransomware attack on Kootenai County exposes resident data" (Mar 2026)
31. **IL** CBS Chicago, "Illinois voter registration database breached" (Jun 2016)
32. **IL** BleepingComputer, "IDHS maps exposed data on ~700,000 residents for years" (Sep 2025)
33. **IN** Meridian Star (AP), "Ransomware halts online posting of county election results" (Nov 2016)
34. **IN** The Record, "Ransomware closes Clay County courthouse; disaster declared" (Jul 2024)
35. **IA** Iowa Capital Dispatch, "Hack at records vendor cuts Iowa counties off from land records" (Dec 2022)
36. **IA** District Administration, "Des Moines Public Schools hit by ransomware" (Jan 2023)
37. **KS** WIBW, "Kansas court system hit by foreign cyberattack" (Oct 2023)
38. **KS** Insurance Journal, "Ransomware attackers steal personal, medical data from Franklin County" (May 2024)
39. **KY** Louisville Public Media, "Pro-Russian DDoS knocks Kentucky elections and courts sites offline" (Oct 2022)
40. **KY** Comparitech, "Ransomware shuts Jefferson County Clerk's offices for a week" (Jul 2024)
41. **LA** Insurance Journal (AP), "Attempted ransomware attack disrupts nearly every state agency" (Nov 2019)
42. **LA** WAFB, "MOVEit breach exposes records of nearly every Louisiana driver" (Jun 2023)
43. **ME** Cybersecurity Dive, "MOVEit breach hits roughly the entire population of Maine" (May 2023)
44. **ME** Bangor Daily News, "Cyberattack forces Bar Harbor offline, water plant controls cut" (Jul 2025)
45. **MD** NBC Washington (AP), "RobbinHood ransomware cripples Baltimore city network" (May 2019)
46. **MD** The Daily Record, "Cyberattack disrupts Maryland transit systems, data lost" (Aug 2025)
47. **MA** SecurityWeek, "Ransomware hits state ferry agency, delaying ticketing" (Jun 2021)
48. **MA** WJAR (NBC 10), "Attleboro intrusion may have exposed SSNs and medical data" (Nov 2025)
49. **MI** The Record, "Cyberattack takes Michigan's largest county offline" (Oct 2024)
50. **MI** Comparitech, "Ransomware gang hits Michigan county on Election Day" (Nov 2024)
51. **MN** The Record, "Medusa leaks Minneapolis schools data after \$1M demand" (Feb 2023)
52. **MN** KTTC, "Cyberattack on St. Paul prompts National Guard activation" (Jul 2025)
53. **MS** Mississippi Secretary of State, "Election Day DDoS knocks Secretary of State sites offline" (Nov 2022)
54. **MS** The Record, "Ransomware forces Vicksburg to shut down city systems" (Oct 2026)
55. **MO** The Record, "MOVEit breach via IBM exposes Missouri Medicaid data" (Jun 2023)
56. **MO** KCTV5, "Ransomware hits Jackson County on election day" (Apr 2024)
57. **MT** CBS News, "School network hack closes 30+ Flathead Valley schools" (Sep 2017)
58. **MT** NBC Montana, "Cyberattack on MSU brings in Montana National Guard" (Apr 2023)
59. **NE** Nebraska Examiner, "Change Healthcare ransomware reaches 575,000+ Nebraskans" (Feb 2024)
60. **NE** Nebraska Attorney General, "Nebraska bank network intrusion" (Jan 2025)
61. **NV** News 3 Las Vegas (KSNV), "Unauthorized party breaches Clark County schools email system" (Oct 2023)
62. **NV** ABC News, "Nevada state offices shut by cyberattack" (Aug 2025)
63. **NH** New Hampshire Public Radio, "Email fraud diverts \$2.3M in Peterborough town funds" (Aug 2021)
64. **NH** Associated Press (via Boston.com), "AI-generated 'Biden' robocall urges NH voters to skip primary" (Jan 2024)
65. **NJ** StateScoop, "Ransomware hits Somerset County weeks before NJ primary" (May 2022)
66. **NJ** The Record, "Malware attack knocks out Passaic County phones and IT" (Mar 2026)
67. **NM** TechTarget, "Ransomware halts Bernalillo County voter registration, jail locks" (Jan 2022)
68. **NM** Government Technology, "Ransomware locks prosecutors out of files statewide" (Mar 2024)
69. **NY** WSKG, "Ransomware days before election puts absentee requests at risk" (Oct 2020)
70. **NY** The Record, "BlackCat ransomware cripples Suffolk County government" (Sep 2022)
71. **NC** NACo County News, "LockCrypt ransomware hits Mecklenburg County; ransom refused" (Dec 2017)
72. **NC** The Record, "Cyberattack leaves Bladen County operating at limited capacity" (Nov 2023)
73. **ND** StateScoop, "Maze ransomware hits fiber provider for ND state network" (Apr 2020)
74. **ND** KFVR-TV, "Ransomware hits Minot water treatment plant server" (2026)
75. **OH** WCBE, "Attackers try to inject code into Ohio SOS website" (Nov 2019)
76. **OH** Infosecurity Magazine, "Rhysida ransomware exposes data of 500,000 Columbus residents" (Jul 2024)
77. **OK** Route Fifty, "Tulsa ransomware shuts city services, leaks 18,000 files" (May 2021)
78. **OK** Oklahoma OMES (official notice), "Unauthorized access to taxpayer data in OkTAP portal" (Dec 2025)
79. **OR** BleepingComputer, "Phishing exposes data of 645,000 Oregon DHS clients" (Jan 2019)
80. **OR** Oregon DOT (official notice), "MOVEit hack exposes 3.5M Oregon driver's license records" (Jun 2023)

81. **PA** 6abc Philadelphia, "Ransomware encrypts Delaware County police and payroll data" (Nov 2020)
82. **PA** Infosecurity Magazine, "Ransomware takes PA Attorney General's office offline" (Aug 2025)
83. **RI** Rhode Island Current, "Medusa ransomware hits Providence schools, demands \$1M" (Sep 2024)
84. **RI** Rhode Island Current, "Brain Cipher breach of RIBridges benefits system exposes 644,000 people" (Dec 2024)
85. **SC** GovTech (via The State), "Nearly 150,000 attempts to penetrate S.C. voter registration system" (Nov 2016)
86. **SC** The Record, "Ransomware attack disrupts Spartanburg County IT and phone systems" (Apr 2023)
87. **SD** South Dakota Searchlight, "Pennington County, S.D., systems knocked out" (Jul 2026)
88. **SD** Dakota News Now, "Cyberattack hits part of Mitchell city computer network" (Aug 2026)
89. **TN** Phys.org (AP), "Election-night results website knocked offline in Knox County" (May 2018)
90. **TN** The Record, "Ransomware attack takes Oak Ridge city network offline" (Mar 2023)
91. **TX** KERA News, "Coordinated ransomware attack hits 23 Texas local governments" (Aug 2019)
92. **TX** Dallas Morning News, "Royal ransomware shuts Dallas courts, disrupts police systems" (May 2023)
93. **UT** BleepingComputer, "University of Utah pays \$457,000 after ransomware attack" (Jul 2020)
94. **UT** Comparitech, "Interlock ransomware steals Box Elder County data, 81,664 notified" (Aug 2025)
95. **VT** Vermont Public, "Joblink breach puts unemployment filers' SSNs at risk" (Mar 2017)
96. **VT** Addison Independent, "Ransomware locks Addison Northwest schools out of servers" (Jan 2025)
97. **VA** UPI, "Ransomware hits Virginia legislature's IT agency, websites" (Dec 2021)
98. **VA** Insurance Journal (Washington Post), "Cyberattack forces Virginia attorney general's office offline" (Feb 2025)
99. **WA** Northwest Public Broadcasting, "Accellion breach may expose 1.6M Washington jobless claims" (Feb 2021)
100. **WA** SecurityWeek, "Rhysida ransomware disrupts Sea-Tac and exposes 90,000 people" (Aug 2024)
101. **WV** The Record, "Cyberattack cancels classes for 20,000 Berkeley County students" (Feb 2023)
102. **WV** The Record, "Cyberattack disrupts Beckley city computer network" (Jan 2024)
103. **WI** WPR, "DHS confirms Russian hackers targeted Wisconsin in 2016" (Sep 2017)
104. **WI** The Record, "Chort ransomware steals data on 67,000 Sheboygan residents" (Oct 2024)
105. **WY** Wyoming Department of Health, "Wyoming health test data posted to public GitHub" (Apr 2021)
106. **WY** Wyoming Public Media, "Court vendor breach exposes Wyoming court users' personal data" (Sep 2026)