

BB2G

BORN BETWEEN 2 GENERALS

CYBER COMMAND · 50 STATES + D.C.

Find the flaw first. Heal before harm.

Americans filed 1,008,597 cybercrime complaints with the FBI in 2025 and reported $20.9 billion in losses. Attackers have reached water plants, hospitals, utilities, airports and election offices in nearly every state. This briefing maps the hot spots and shows how BB2G code scans itself for weaknesses, quarantines what it finds and repairs itself before anyone is hurt.

BORN BETWEEN 2 GENERALS, LLC · CYBER COMMAND UPDATED NOV. 10, 2026 CYBERMAP.BORNBETWEEN2GENERALS.COM

EXECUTIVE SUMMARY · THREAT MAP

Where the attacks are landing

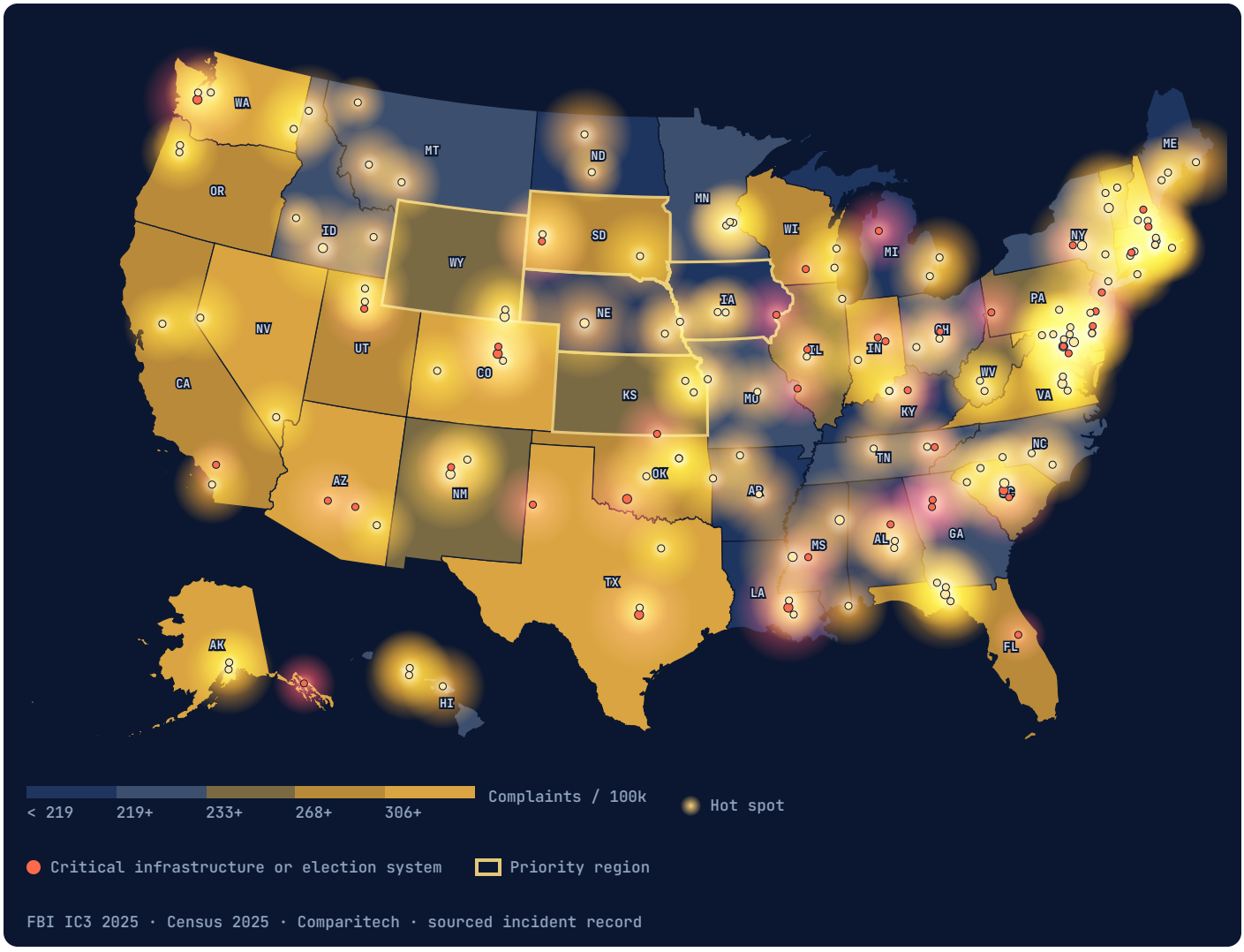
States are shaded by FBI cybercrime complaints per 100,000 residents. Each glow is a documented attack on a hospital, utility, government office, school or election system; red marks critical infrastructure and election systems.

1,008,597
Cybercrime complaints filed with the FBI in 2025

$20.9B
Reported losses in 2025, the highest on record

161
Incidents documented across 51 jurisdictions

1,756
Confirmed ransomware attacks on U.S. organizations, 2018 – mid-2022



Water is in the crosshairs

Hackers reached water and wastewater systems in Aliquippa, Pa., Muleshoe, Texas, Tipton, Ind., Arkansas City, Kan., Childersburg, Ala., and Rapid City, S.D. Iran-

Hospitals go dark

Ransomware forced ambulance diversions or paper charts at Kettering Health, Ascension, Ardent, Prospect Medical and AnMed, among others.

The priority region

Nebraska, Iowa, South Dakota, Kansas and Wyoming residents lost $392 million to cybercrime in 2025; Muscatine, Arkansas City and Rapid City utilities were hit.

and Russia-linked groups were behind four of them.

LATEST · SEPT. – NOV. 2026

What hit this fall

Recent attacks and national advisories, newest first. Red cards hit critical infrastructure or election systems.

CRITICAL INFRASTRUCTURE AND ELECTION SYSTEMS

NEW Nov 2026 · Colorado

Colorado election results website down about 45 minutes on election night

The state's public election results site went down around 7 p.m. Nov. 3 and returned about 45 minutes later with a CAPTCHA. Vendor SOE Software blamed unusually high automated traffic from results-scraping entities, and officials said ballot returns and results were not affected.

Colorado Politics

NEW Nov 2026 · Washington

Washington Secretary of State website hit by cyberattack

Increased traffic over several days made some Secretary of State web pages temporarily unavailable; the pages were restored and the incident is under investigation. A spokesperson said bots caused the surge, and county tabulation machines are not internet-connected and were not affected.

KOMO News

NEW Nov 2026 · South Carolina

SCVotes voter lookup tools fail intermittently on Election Day

Some voters could not get sample ballots and precinct details from the SCVotes website on the morning of Nov. 3. A commission spokesperson cited an intermittent issue with voter-facing features and said capacity was being added to handle traffic.

WCSC Live 5 News

NEW Nov 2026 · Oklahoma

Technical issues delay results reporting in two Oklahoma counties

Comanche and Cleveland counties had separate technical issues that temporarily delayed transmission of results to the State Election Board on election night. Cleveland used a backup upload system and Comanche entered results manually; the state said the results themselves were not affected.

Oklahoma State Election Board

NEW Oct 2026 · Texas

Software glitch backlogs nearly 600,000 Texas voter registrations

Nearly 600,000 voter registration applications were backlogged ahead of early voting. A lawsuit by voting rights groups blames a glitch in software run by the Texas Department of Public Safety.

Political Wire

NEW Oct 2026 · Louisiana

Database error wrongly marks 67,000 Louisiana voters inactive

About 67,000 voters were mistakenly marked inactive during routine database maintenance, and the office restored them to active status later that day. The office blamed human error and said no one's eligibility or ability to vote was affected.

The Center Square / Just The News

NATIONAL ADVISORIES

NEW Nov 2026 · national

CIS Election Day summary: probing, password guessing, DDoS-style traffic

CIS reported one election office saw scans and failed intrusion attempts, an election agency saw failed password-guessing from a single IP address, and offices saw automated traffic surges on web pages. It said most incidents were resolved quickly and no foreign adversary information operations were reported.

Center for Internet Security

NEW Nov 2026 · national

Election offices report failed hacking attempts on Election Day

An unnamed election office reported probing and failed break-in attempts on Nov. 3, and an election-related agency saw failed login-guessing from one IP address that several offices also observed. The EI-ISAC said that as of 9:30 p.m. EST it had no reports of foreign influence operations.

Nextgov/FCW

NEW Oct 2026 · national

FBI warns of midterm scams including fake voter registration pages

The FBI issued a public service announcement warning scammers could exploit the 2026 midterms with fake donation pages, AI-cloned candidate voices, and texts linking to fake state voter registration sites that harvest personal data.

Help Net Security

NEW Oct 2026 · national

Cyber incident at contractor halts federal bankruptcy notices nationwide

A cybersecurity incident at BAE Systems, which runs the Bankruptcy Noticing Center for the federal judiciary, halted production and delivery of bankruptcy notices from Oct. 9. The BNC websites remained offline as of Oct. 16, while courts kept accepting filings.

CyberScoop

GOVERNMENT, SCHOOLS AND HEALTH

NEW 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.

The Record

NEW Oct 2026 · Nebraska

North Platte and Lincoln County, Neb., knocked offline

A cyberattack on Oct. 9 knocked out internet and systems for the City of North Platte and Lincoln County. The governor declared an emergency and the Nebraska National Guard cyber team deployed; the mayor later said a stolen employee password caused the attack.

Government Technology

NEW Oct 2026 · District of Columbia

FEC takes e-filing system offline after reported hacking attempt

The FEC's electronic filing system went offline late Oct. 26 after an official warned that a bad actor was attempting to breach FEC systems and web-facing services were shut down. The FEC confirmed the disruption but has not confirmed a successful breach.

eSecurity Planet

NEW Oct 2026 · Mississippi

Attack on web provider disrupts about 70 Mississippi government websites

A cyberattack on Jackson-based website provider U.S.NEXT disrupted about 70 government websites. In West Point, residents saw errors when trying to pay water and electric bills online.

WLOX

NEW Oct 2026 · South Carolina

Columbia, S.C. confirms ransomware attack disrupting online services

The city confirmed a ransomware attack that disrupted online services including its MyColaSC reporting system, parks reservations and GIS. SLED is investigating, and police, fire, 911 and water service stayed operational.

ABC News 4

NEW Oct 2026 · Maryland

Anne Arundel County confirms breach as Rhysida demands $2 million

The county confirmed an unauthorized actor accessed a small number of systems in August and copied some files. The Rhysida ransomware gang claimed the attack, demanded $2 million and threatened to leak 2.6 TB of documents.

The Record

NEW Oct 2026 · Virginia

Richmond Public Schools offline for over a week after cyber incident

After suspicious activity was detected Oct. 21, the district took internet access offline across all schools, limiting phones, email and online learning tools. The FBI and Virginia State Police are working with the district.

WTVR CBS 6

NEW Oct 2026 · New York

Ransomware cancels classes in Oneonta City School District

The district discovered the incident Oct. 22, later confirmed ransomware, and canceled classes while outside experts investigated. It was not yet known whether personal records were compromised.

Cybernews

NEW Oct 2026 · Idaho

Ransomware attack closes Jerome School District for two days

A ransomware attack hit the district Oct. 17, closing schools for two days; the district refused to pay on FBI guidance. The superintendent said some data from local machines was compromised.

Government Technology

NEW Oct 2026 · Florida

Florida student aid website breach may affect 4.9 million people

FLDOE announced unauthorized criminal access to the Florida Student Financial Aid website. Exposed data may include Social Security numbers, names, birth dates and addresses.

WWSB ABC7

NEW Oct 2026 · New Mexico

Cyberattack diverts ambulances from University of New Mexico Hospital

A cyberattack detected Oct. 26 led to ambulance diversions, canceled clinic appointments and procedures, and canceled health-school classes. The BYOD extortion group claimed it compromised 36,000 machines; UNM HSC said impact was limited to some end-user devices.

Help Net Security

NEW Oct 2026 · Vermont

Slate Valley school district refuses ransom after data breach

Hackers accessed business documents and employee personal information in a September breach and demanded a ransom. On Oct. 2 the district said its board declined to pay on legal advice.

WCAX

NEW Sep 2026 · Wyoming

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.

Wyoming Public Media

SAFE CODE · SELF-SCAN · SELF-HEAL

Code that hunts its own weaknesses and repairs itself

Most breaches start with a known flaw nobody patched or a new one nobody saw. BB2G systems scan themselves on every build and every day, contain anything that behaves wrong, and restore a verified good state in seconds.

01
Scan
Every build: software bill of materials, dependency and secret scans. Every day: PATCH ROLL checks the CISA Known Exploited Vulnerabilities list.

02
Detect
Zero-day behavior sandbox runs unverified packages in short-lived memory containers and kills them on a kernel read or reverse shell.

03
Contain
A suspect port or service moves to a quarantine network; normal traffic reroutes around it.

04
Repair
resilience-daemon-v2 restarts a failed service within 3 seconds and rebuilds altered files from a hash-verified, write-once copy.

05
Verify
Hashes, tests and a two-key approval confirm the repair before the service rejoins.

06
Seal
A signed receipt goes to an append-only ledger, and the finding becomes a new scan rule.

↻ Every repair feeds the next scan. Anything it can't verify fails closed and pages a person.

SAFE-CODING RULES BUILT IN

SECURE BY DESIGN
Built to CISA Secure by Design and the NIST Secure Software Development Framework.

SIGNED EVERYTHING
Signed commits, signed builds and a software bill of materials for every release.

NO SECRETS IN CODE
Keys live in vaults. Leaked tokens found in public code or breach dumps are revoked automatically.

GATES BEFORE MERGE
Static analysis, dependency checks and tests must pass before code can merge.

RESPONSIBLE DISCLOSURE
A new flaw found in someone else's product goes to the vendor and CISA through coordinated disclosure.

BLAST-RADIUS REHEARSAL
Infrastructure changes run in a throwaway copy first to show exactly what they would touch.

CYBER COMMAND · OPERATION STRONGROOM

Confirm in milliseconds, contain in seconds, decide with two keys

The command desk fuses network, device and open-source signals, then runs a fixed four-phase response. People make the final call; the system buys them time.

1 Confirm
Signals are scored against each site's normal baseline; a high composite score escalates in under 50 milliseconds.

2 Quarantine
Compromised ports drop into a dead-end network while suspicious connections are routed to a decoy for evidence.

3 Mirror
Fresh 3-2-1 copies of critical state are written to separate media and an encrypted off-site link.

4 Lock
Administrative changes freeze until two hardware keys approve the reset.

5 Trace
TRACK-BACK documents the intrusion path for law enforcement. BB2G traces; it never hacks back.

6 Report
A sealed incident packet with timeline and evidence goes to the owner, CISA and insurers.

STANDING DEFENSES

PICKET · STAND-TO
Continuous watch of public signals, certificates, leaked credentials and exposed services.

PATCH ROLL
Known exploited vulnerabilities patched on CISA's deadline, with proof for each system.

LATCHKEY
FIDO2 hardware keys for every privileged account; phishing can't steal them.

GATEHOUSE
Ten-point vetting for every vendor before it touches a network.

CIS-AUTOSHIELD
CIS benchmark hardening applied and re-checked automatically.

OT ISOLATION
Water, power and building controls separated from office networks and the internet.

TRACE BACK, NEVER HACK BACK Every response stays defensive and lawful. Evidence is preserved for the people with authority to act on it.

WHY DEFENSES FAIL QUIETLY

Twenty steps at 95% means two releases in three ship a flaw

A release passes through code, review, dependencies, build, deploy, monitoring, patching and backup. If each step is right 95% of the time, the whole chain is clean only 36% of the time, and real systems have far more than 20 steps.

CHAIN LENGTH	95% PER STEP, NO CHECKS	99% PER STEP, NO CHECKS	95% PER STEP, BB2G CHECKS	99% PER STEP, BB2G CHECKS
10 steps	59.9%	90.4%	99.5%	99.90%
20 steps	35.8%	81.8%	99.0%	99.80%
50 steps	7.7%	60.5%	97.5%	99.50%
100 steps	0.6%	36.6%	95.1%	99.00%
200 steps	0.0%	13.4%	90.5%	98.02%

Chance the chain finishes with no undetected error. With BB2G, each step is gated: a check catches 99% of errors and stops the release instead of shipping it.

A SOFTWARE RELEASE · GOLD STEPS ARE BB2G GATES

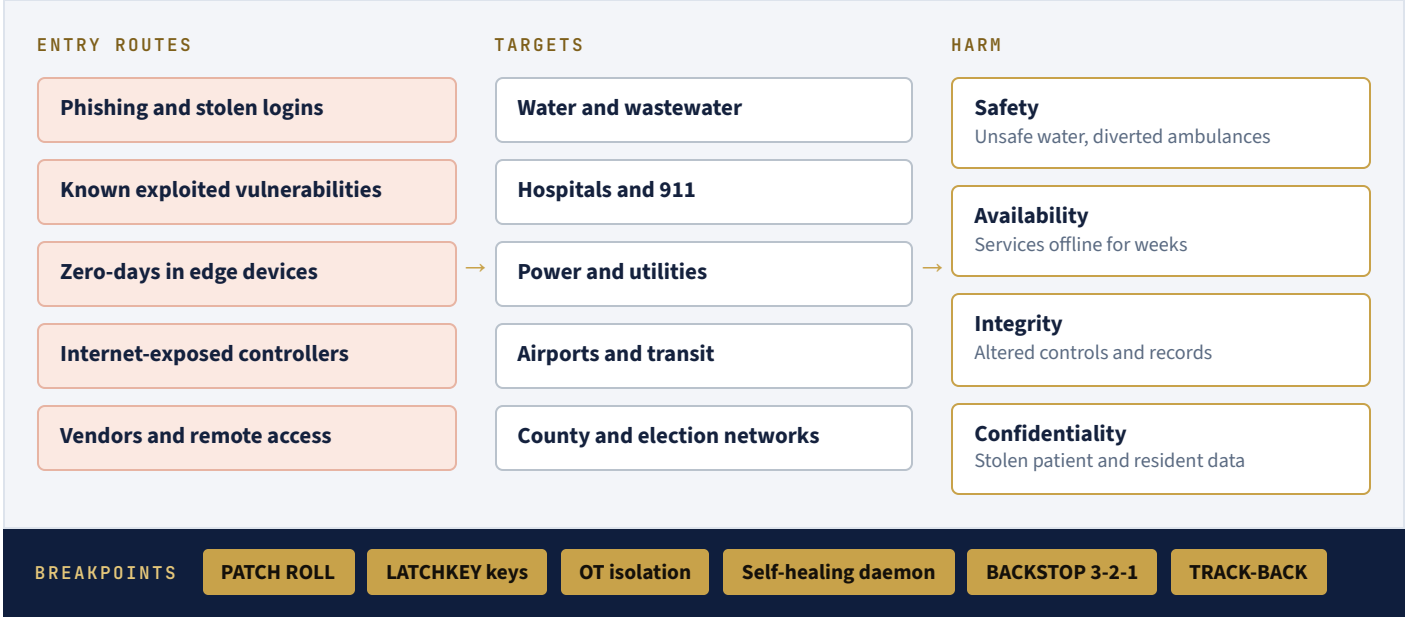
Code written · Peer review · **Static analysis** · Dependencies · SBOM · **KEV and CVE check** · Build · Signed · Tests · **Sandbox detonation** · Staging · Blast-radius rehearsal · **Two-key approval** · Deploy · Monitor · Patch · Backup · **Restore drill** · Incident drill · Recover

FAIL CLOSED A gate that finds a problem stops the line. Shipping late is recoverable; shipping a known flaw to a water plant isn't.

ATTACK PATHWAY

Route to harm, and where to break it

How attackers get from first access to physical and public harm, and the controls that stop them.



NATIONAL RANKINGS

How every state compares

Rank 1 has the highest FBI cybercrime complaint rate per resident (2025). Priority region shaded.

RANK	JURISDICTION	REGION	PER 100K	COMPLAINTS	LOSSES	LOSS / RESIDENT	RANSOMWARE	INCIDENTS
1	**District of Columbia**	South	449	3,113	$97.4M	$140.37	7	4
2	**Alaska**	West	434	3,202	$40.0M	$54.22	6	3
3	**Nevada**	West	407	13,366	$302.2M	$92.08	17	2
4	**Arizona**	West	379	28,868	$630.7M	$82.73	22	3
5	**Massachusetts**	Northeast	321	22,936	$410.9M	$57.44	85	3
6	**Washington**	West	320	25,619	$458.2M	$57.26	47	4
7	**Colorado**	West	314	18,847	$355.0M	$59.05	30	4
8	**Maryland**	South	310	19,430	$390.2M	$62.29	32	4
9	**New Hampshire**	Northeast	309	4,374	$59.3M	$41.89	10	3
10	**Texas**	South	309	97,912	$1.83B	$57.57	130	4
11	**Florida**	South	306	71,843	$1.60B	$68.03	90	4
12	**Indiana**	Midwest	298	20,777	$233.0M	$33.42	36	3
13	**California**	West	296	116,414	$3.67B	$93.37	172	3
14	**Oregon**	West	292	12,477	$193.2M	$45.21	20	2
15	**Delaware**	South	291	3,089	$62.0M	$58.51	5	3
16	**Oklahoma**	South	290	11,964	$131.9M	$31.99	25	4
17	**Virginia**	South	285	25,314	$476.1M	$53.62	32	3
18	**Utah**	West	280	9,903	$195.4M	$55.22	14	3
19	**Wisconsin**	Midwest	279	16,680	$194.2M	$32.52	27	3
20	**South Dakota**	Midwest	269	2,514	$51.5M	$55.02	3	3
21	**New Mexico**	West	268	5,688	$85.6M	$40.26	19	3
22	**Kansas**	Midwest	266	7,927	$147.3M	$49.49	14	3
23	**South Carolina**	South	264	14,699	$264.1M	$47.41	20	5
24	**Wyoming**	West	264	1,552	$25.8M	$43.87	3	2
25	**Connecticut**	Northeast	263	9,714	$219.5M	$59.51	40	3
26	**Illinois**	Midwest	259	32,977	$535.3M	$42.08	79	3
27	**Vermont**	Northeast	245	1,580	$26.6M	$41.21	3	3
28	**Rhode Island**	Northeast	242	2,700	$72.0M	$64.57	7	3
29	**Pennsylvania**	Northeast	239	31,154	$537.8M	$41.18	68	3
30	**West Virginia**	South	238	4,209	$92.6M	$52.46	6	3

RANK	JURISDICTION	REGION	PER 100K	COMPLAINTS	LOSSES	LOSS / RESIDENT	RANSOMWARE	INCIDENTS
31	**Minnesota**	Midwest	233	13,595	$248.9M	$42.69	27	3
32	**Hawaii**	West	232	3,328	$106.4M	$74.29	7	3
33	**Ohio**	Midwest	232	27,626	$421.3M	$35.40	58	3
34	**North Carolina**	South	232	25,940	$431.6M	$38.54	55	3
35	**Georgia**	South	230	25,936	$534.6M	$47.30	66	3
36	**Montana**	West	229	2,618	$53.2M	$46.47	10	3
37	**New York**	Northeast	226	45,255	$1.23B	$61.31	116	4
38	**Missouri**	Midwest	225	14,087	$233.9M	$37.31	44	3
39	**Tennessee**	South	222	16,261	$269.2M	$36.80	26	3
40	**Idaho**	West	221	4,479	$88.7M	$43.71	13	4
41	**Michigan**	Midwest	219	22,191	$381.1M	$37.63	45	3
42	**New Jersey**	Northeast	216	20,648	$660.4M	$69.17	56	3
43	**Kentucky**	South	204	9,414	$119.7M	$25.98	15	3
44	**Maine**	Northeast	204	2,888	$56.5M	$39.96	16	3
45	**Arkansas**	South	198	6,161	$102.5M	$32.92	13	3
46	**Alabama**	South	191	9,936	$167.2M	$32.20	27	3
47	**Louisiana**	South	187	8,623	$105.4M	$22.83	32	3
48	**Nebraska**	Midwest	185	3,724	$71.8M	$35.60	16	3
49	**North Dakota**	Midwest	177	1,418	$37.9M	$47.37	3	2
50	**Mississippi**	South	172	5,084	$77.4M	$26.19	19	4
51	**Iowa**	Midwest	168	5,436	$95.5M	$29.50	20	3

INCIDENT RECORD · 2016 – NOV. 2026

What has already happened

Documented cyberattacks on hospitals, utilities, transportation, government, schools and election systems, newest first, each linked to its source.

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
2026			
Nov 2026	NEW **Colorado** CRITICAL	**Colorado election results website down about 45 minutes on election night** The state's public election results site went down around 7 p.m. Nov. 3 and returned about 45 minutes later with a CAPTCHA. Vendor SOE Software blamed unusually high automated traffic from results-scraping entities, and officials said ballot returns and results were not affected.	~45-minute outage Colorado Politics
Nov 2026	NEW **Washington** CRITICAL	**Washington Secretary of State website hit by cyberattack** Increased traffic over several days made some Secretary of State web pages temporarily unavailable; the pages were restored and the incident is under investigation. A spokesperson said bots caused the surge, and county tabulation machines are not internet-connected and were not affected.	Some pages temporarily down KOMO News
Nov 2026	NEW **South Carolina** CRITICAL	**SCVotes voter lookup tools fail intermittently on Election Day** Some voters could not get sample ballots and precinct details from the SCVotes website on the morning of Nov. 3. A commission spokesperson cited an intermittent issue with voter-facing features and said capacity was being added to handle traffic.	Voter lookup features WCSC Live 5 News
Nov 2026	NEW **Oklahoma** CRITICAL	**Technical issues delay results reporting in two Oklahoma counties** Comanche and Cleveland counties had separate technical issues that temporarily delayed transmission of results to the State Election Board on election night. Cleveland used a backup upload system and Comanche entered results manually; the state said the results themselves were not affected.	Two counties Oklahoma State Election Board
Oct 2026	NEW **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
Oct 2026	NEW **Nebraska** PRIORITY	**North Platte and Lincoln County, Neb., knocked offline** A cyberattack on Oct. 9 knocked out internet and systems for the City of North Platte and Lincoln County. The governor declared an emergency and the Nebraska National Guard cyber team deployed; the mayor later said a stolen employee password caused the attack.	City + county offline Government Technology
Oct 2026	NEW **District of Columbia**	**FEC takes e-filing system offline after reported hacking attempt** The FEC's electronic filing system went offline late Oct. 26 after an official warned that a bad actor was attempting to breach FEC systems and web-facing services were shut down. The FEC confirmed the disruption but has not confirmed a successful breach.	Nationwide campaign filings eSecurity Planet
Oct 2026	NEW **Texas** CRITICAL	**Software glitch backlogs nearly 600,000 Texas voter registrations** Nearly 600,000 voter registration applications were backlogged ahead of early voting. A lawsuit by voting rights groups blames a glitch in software run by the Texas Department of Public Safety.	~600,000 applications Political Wire

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Oct 2026	NEW **Louisiana** CRITICAL	**Database error wrongly marks 67,000 Louisiana voters inactive** About 67,000 voters were mistakenly marked inactive during routine database maintenance, and the office restored them to active status later that day. The office blamed human error and said no one's eligibility or ability to vote was affected.	~67,000 voters The Center Square / Just The News
Oct 2026	NEW **Mississippi**	**Attack on web provider disrupts about 70 Mississippi government websites** A cyberattack on Jackson-based website provider U.S.NEXT disrupted about 70 government websites. In West Point, residents saw errors when trying to pay water and electric bills online.	~70 government websites WLOX
Oct 2026	NEW **South Carolina**	**Columbia, S.C. confirms ransomware attack disrupting online services** The city confirmed a ransomware attack that disrupted online services including its MyColaSC reporting system, parks reservations and GIS. SLED is investigating, and police, fire, 911 and water service stayed operational.	Several online services ABC News 4
Oct 2026	NEW **Maryland**	**Anne Arundel County confirms breach as Rhysida demands $2 million** The county confirmed an unauthorized actor accessed a small number of systems in August and copied some files. The Rhysida ransomware gang claimed the attack, demanded $2 million and threatened to leak 2.6 TB of documents.	2.6 TB claimed The Record
Oct 2026	NEW **Virginia**	**Richmond Public Schools offline for over a week after cyber incident** After suspicious activity was detected Oct. 21, the district took internet access offline across all schools, limiting phones, email and online learning tools. The FBI and Virginia State Police are working with the district.	District-wide WTVR CBS 6
Oct 2026	NEW **New York**	**Ransomware cancels classes in Oneonta City School District** The district discovered the incident Oct. 22, later confirmed ransomware, and canceled classes while outside experts investigated. It was not yet known whether personal records were compromised.	~1,700 students Cybernews
Oct 2026	NEW **Idaho**	**Ransomware attack closes Jerome School District for two days** A ransomware attack hit the district Oct. 17, closing schools for two days; the district refused to pay on FBI guidance. The superintendent said some data from local machines was compromised.	Schools closed 2 days Government Technology
Oct 2026	NEW **Florida**	**Florida student aid website breach may affect 4.9 million people** FLDOE announced unauthorized criminal access to the Florida Student Financial Aid website. Exposed data may include Social Security numbers, names, birth dates and addresses.	~4.9 million people WWSB ABC7
Oct 2026	NEW **New Mexico**	**Cyberattack diverts ambulances from University of New Mexico Hospital** A cyberattack detected Oct. 26 led to ambulance diversions, canceled clinic appointments and procedures, and canceled health-school classes. The BYOD extortion group claimed it compromised 36,000 machines; UNM HSC said impact was limited to some end-user devices.	Hospital and clinics Help Net Security
Oct 2026	NEW **Vermont**	**Slate Valley school district refuses ransom after data breach** Hackers accessed business documents and employee personal information in a September breach and demanded a ransom. On Oct. 2 the district said its board declined to pay on legal advice.	Employee data WCAX

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Sep 2026	NEW **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	**Childersburg, AL** CRITICAL	**Iran-linked campaign hits Childersburg utility control network** Attackers targeted the utility's computerized monitoring and control network, involving a programmable logic controller, and officials temporarily disconnected the system. No significant service disruption was reported.	Water, sewer, gas utility Security Affairs
Jul 2026	**Anderson, SC**	**Malware takes AnMed hospital network to paper charts** Malware knocked out phones, internet and many computer systems at all AnMed hospital locations, forcing staff onto paper records and handwritten orders. Medical group offices and imaging closed while ERs stayed open.	All hospital locations FOX Carolina
Jul 2026	**Rapid City, SD** CRITICAL PRIORITY	**Hackers target Rapid City wastewater lift station** Attackers tried to interfere with one of the city's wastewater lift stations during the summer 2026 wave of attacks on U.S. water systems. The city isolated the affected systems and said drinking water and public safety were not affected.	One lift station Newsweek
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
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

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
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** KFYR-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	**Anchorage, AK**	**Anchorage health center takes systems offline after breach** The health center confirmed a data security incident on its network and took affected systems offline. A hacker group claimed it accessed records of 60,000 patients, which was not verified.	**Up to 60,000 claimed** Becker's Hospital Review
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
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

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Jul 2025	**Washington, DC** CRITICAL	**SharePoint zero-day used to breach U.S. nuclear weapons agency** Attackers exploited the ToolShell SharePoint zero-day chain to access Energy Department networks, including NNSA, starting July 18. DOE said a very small number of systems were affected and no classified data was reported compromised.	**Small number of systems** BleepingComputer
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	**Lewiston, ME**	**Cyber incidents at Lewiston hospitals force ambulance diversions** Central Maine Medical Center shut down its technology systems on June 1, and nearby St. Mary's also had a cyber incident. Both diverted ambulances and patients waited for surgeries, prescriptions and imaging.	**2 Lewiston hospitals** EMS1 / Morning Sentinel
Jun 2025	**Arizona** CRITICAL	**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	**Nashua, NH**	**Cyberattack forces Covenant Health offline, hitting Nashua hospital services** Covenant Health cut off access to all of its data systems after a cyberattack detected May 26, 2025. At St. Joseph Hospital in Nashua, phone and internet outages left some services unavailable, and lab work was limited to the main campus.	**Systemwide data shutdown** The Record
May 2025	**Dayton, OH**	**Interlock ransomware knocks Kettering Health's 14 hospitals offline** Starting May 20, 2025, the attack took down phones and the electronic health record system across the network. Several facilities canceled elective procedures and some ambulances were diverted, with outages lasting about two weeks.	**14 medical centers** The Record
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
Mar 2025	**Little Rock, AR**	**EHR vendor breach exposes Arkansas Heart Hospital patient records** Attackers accessed patient medical records in a vendor's systems used during the hospital's move to a new electronic records system. Patients treated from 2022 to January 2025 may be affected.	**Three years of patients** ClaimDepot

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Feb 2025	**Colfax, WA**	**Intruders take down Whitman Hospital's internal systems** The rural hospital found on Feb. 28, 2025 that its systems had been infiltrated by an unknown attacker. Internal systems were still down days later and appointments faced delays, though the hospital and clinics stayed open.	**Hospital and clinics** DataBreaches.net
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	**Frederick, MD**	**Ransomware forces Frederick Health to divert ambulances** Ransomware took electronic health records and e-prescribing offline, and staff reverted to paper. Ambulances were diverted and the hospital's village laboratory suspended operations.	**Ambulances diverted** Daily Security Review
Jan 2025	**Pinehurst, NC**	**Cyberattack shuts Pinehurst radiology practice for over a month** A January 2025 cyberattack closed the Sandhills-region practice for more than a month. With scheduling down, patients could not book mammograms or ultrasounds, and PET and MRI patients were sent to an affiliated provider.	**Practice closed 1+ month** HIPAA Journal
Jan 2025	**Nebraska** PRIORITY	**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			
Dec 2024	**Salt Lake City, UT** CRITICAL	**Ransomware hits network controlling Salt Lake City airport systems** Attackers compromised administrator accounts on a network that manages airport controls such as ventilation and paging, then deployed ransomware that locked staff out of several systems. State auditors said critical systems were put at risk.	**Multiple airport systems** KSL
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	**Bainbridge, GA**	**Embargo ransomware knocks out Bainbridge hospital's health records** Ransomware cut access to the hospital's electronic health records, forcing staff onto paper and lengthening patient waits. The Embargo gang claimed the attack and threatened to leak 1.15 TB of data.	**1.15 TB claimed stolen** The Record
Nov 2024	**Michigan** CRITICAL	**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	**Camden, NJ** CRITICAL	**Hackers breach largest U.S. water utility; billing and portal shut down** Camden-based American Water found unauthorized activity on Oct. 3, 2024, and disconnected systems. Its MyWater portal and billing were paused. The company said its water and wastewater operations were not affected.	**14M+ people served** NJBIZ

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Oct 2024	**Colorado** CRITICAL	**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** CRITICAL	**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	**Arkansas City, KS** CRITICAL PRIORITY	**Cyberattack forces Kansas water plant to manual operations** A cybersecurity incident at the city's water treatment facility forced it to switch to manual operations. The city said water service and quality were not affected.	**One treatment plant** SecurityWeek
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	**Port Huron, MI**	**Cyberattack on McLaren diverts ambulances, postpones care** A criminal cyberattack hit McLaren's 13 Michigan hospitals, postponing some appointments, treatments and tests. Ambulances were temporarily diverted from McLaren Port Huron Hospital.	**13 hospitals** Chief Healthcare Executive
Aug 2024	**Anaconda, MT**	**Meow ransomware gang claims attack on Anaconda critical access hospital** Attackers got into the 25-bed critical access hospital's network on Aug. 10-12, 2024, disrupting access to some IT systems. Meow claimed it stole 540 GB and demanded $120,000. The hospital later confirmed that 21,243 people's SSNs and medical data were exposed.	**21,243 people affected** Comparitech
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
Jul 2024	**Dover, DE**	**Rhysida ransomware gang breaches Bayhealth, 497,000 affected** Attackers were inside Bayhealth's network from July 27 to 31, 2024, and stole files including data used to run its facilities. The Rhysida gang demanded 25 bitcoins and the breach affected 497,047 people.	**497,047 people** GovInfoSecurity

DATE	JURISDICTION	WHAT HAPPENED	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	**Delta County, CO**	**Delta Health cyberattack exposes data of 148,363 people** Attackers breached the rural hospital district's network in late May 2024. The breach affected 148,363 people, and no group has claimed it.	**148,363 people** DataBreaches.net
May 2024	**Wailuku, HI**	**Alleged LockBit attack shuts Maui health center two weeks** The health center serving about 12,000 patients was shut down for more than two weeks in May 2024. The LockBit ransomware group allegedly claimed the attack.	**12,000 patients** Hawaii News Now
May 2024	**Nashville, TN**	**Ascension ransomware puts Saint Thomas ERs on ambulance diversion** An attack starting May 8, 2024, which has been linked to Black Basta, took down electronic health records and ordering systems. Some Tennessee emergency rooms went on diversion, and imaging and testing were delayed.	**Statewide Saint Thomas network** WPLN
May 2024	**Milwaukee, WI**	**Ascension cyberattack slows care at Milwaukee hospitals** After Ascension detected unusual network activity on May 8, 2024, its electronic records and MyChart went offline. Milwaukee-area patients missed CT scans and mammograms and could not refill prescriptions, and St. Francis Hospital switched to paper records.	**140 hospitals, 19 states** PBS Wisconsin
May 2024	**Kansas** PRIORITY	**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	**Tipton, IN** CRITICAL	**Russia-linked hacktivists target Tipton wastewater plant** The Cyber Army of Russia posted video it said showed hackers interacting with the plant's systems, prompting an investigation. The utility said the plant stayed operational with minimal disruption.	**Minimal disruption** The Record
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

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
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	**Chicago, IL**	**Rhysida ransomware takes Lurie Children's network offline** The children's hospital took its whole network offline, canceled some appointments and elective surgeries, and ran on manual processes for weeks. Rhysida sought $3.4 million for the stolen data.	**$3.4M data sale demand** The Record
Feb 2024	**Eden Prairie, MN**	**Attack on radiology firm disrupts reads for 22 hospitals** A suspected cyberattack halted parts of the radiology outsourcing firm's operations, hitting a large share of Allina Health partner clinics. One hospital reportedly diverted stroke patients.	**22 affiliated hospitals** AuntMinnie
Feb 2024	**Nebraska** PRIORITY	**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
Jan 2024	**Muscatine, IA** CRITICAL PRIORITY	**Ransomware hits Muscatine power and water utility** Ransomware hit the utility's corporate network, knocking internet service out for eight hours and exposing data on 36,955 people. The utility said power plant control systems were never at risk.	**36,955 people** The Record
Jan 2024	**Muleshoe, TX** CRITICAL	**Russia-linked hackers cause Muleshoe water system to overflow** Attackers caused the town's water system to overflow until officials shut it down and ran it manually. Mandiant linked the attacks to CyberArmyofRussia_Reborn. The city said disinfection was not affected.	**Small-town water system** Fortune
Jan 2024	**Georgia** CRITICAL	**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** CRITICAL	**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

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Nov 2023	**Oceanside, CA**	**Cyberattack forces Oceanside hospital to divert ambulances** The hospital declared an internal disaster and activated its command center after a cyberattack. Ambulances were diverted while the emergency room stayed open for walk-in patients.	Ambulances diverted Becker's Hospital Review
Nov 2023	**Littleton, MA** CRITICAL	**Chinese Volt Typhoon hackers lurked in Littleton utility 300 days** Chinese state-backed Volt Typhoon hackers were inside the utility's network from about February 2023 until the FBI alerted it in November. They sought data on grid operating procedures and layout.	300-day intrusion The Record
Nov 2023	**Tulsa, OK**	**Ransomware forces Tulsa-area Hillcrest hospitals to divert ER patients** A Nov. 23, 2023 ransomware attack on Ardent Health took its network and patient documentation systems offline. Hillcrest hospitals and clinics in the Tulsa area rescheduled non-emergency procedures and diverted some emergency patients.	10 Oklahoma facilities KGOU
Nov 2023	**Aliquippa, PA** CRITICAL	**Iran-backed Cyber Av3ngers seize control of Aliquippa water booster station** Attackers took control of a Unitronics-based system at a booster station that regulates water pressure for Raccoon and Potter townships, setting off an alarm. Officials disabled the system and said the drinking water was not at risk.	One booster station CBS News Pittsburgh
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	**Safford, AZ**	**Cyberattack disrupts Safford hospital's communication systems** An attack disrupted the hospital's communication and information systems, and staff worked to restore access to patient information. The hospital said patient impact was limited.	Regional hospital The Record
Oct 2023	**St. Louis, MO** CRITICAL	**Cyberattack cuts St. Louis paratransit to dialysis trips only** A cyberattack took down Call-A-Ride's phones and computer network. Only pre-scheduled, life-critical dialysis rides ran the next day while scheduling software was restored.	Paratransit service cut The Record
Oct 2023	**Kingston, NY**	**Cyber threat forces three Hudson Valley facilities to divert ambulances** A potential cybersecurity threat and IT outage led HealthAlliance Hospital, Margaretville Hospital and Mountainside Residential Care Center to divert ambulances from Oct. 14 to 17, 2023. Phone, email and internet service went offline until systems were restored Oct. 21.	3 facilities on diversion The Record
Oct 2023	**District of Columbia** CRITICAL	**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)

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Aug 2023	**Manchester, CT**	**Prospect Medical attack closes two Connecticut ERs** Emergency departments at Manchester Memorial and Rockville General closed for much of a day and ambulances were diverted. Elective surgeries and outpatient visits were suspended, and Waterbury Hospital moved to paper records.	**3 Connecticut hospitals** Connecticut Public
Aug 2023	**Pascagoula, MS**	**Ransomware takes Singing River hospitals offline, slows labs** The Gulf Coast system took its computers offline and moved its three hospitals and clinics to paper records. Lab processing and radiology results were delayed and the patient app went offline.	**3 hospitals, 10 clinics** Chief Healthcare Executive
Aug 2023	**Providence, RI**	**Prospect Medical cyberattack hits two Rhode Island hospitals** A cyberattack on parent company Prospect Medical Holdings, which began Aug. 3, 2023, hit Roger Williams Medical Center and Fatima Hospital. Prospect said the attack led its network to shut down emergency rooms and redirect ambulances.	**2 RI hospitals** NewsRadio WPRO
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 Cl0p 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
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; Cl0p claimed the MOVEit attack.	**3.5M records** Oregon DOT (official notice)
May 2023	**Idaho Falls, ID**	**Cyberattack diverts ambulances from Idaho Falls hospital** Malware hit the hospital, forcing ambulances to be diverted to nearby hospitals and some connected clinics to close. The emergency department stayed open.	**Ambulances diverted** The Record
May 2023	**Louisville, KY**	**BlackCat ransomware forces Norton hospitals onto paper records** Norton took its systems offline and hospitals reverted to paper records, with some procedures rescheduled and imaging results delayed. AlphV/BlackCat claimed the attack, which affected about 2.5 million people.	**2.5 million people** The Record
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

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
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	**Montgomery, WV**	**D#nut ransomware hits Montgomery General, EHR pulled offline** Ransomware deployed around March 1, 2023 led the hospital to take its electronic medical record system offline as a precaution. The gang demanded $750,000, and the hospital did not pay. The hospital said patient care was not affected.	**$750K ransom demand** Healthcare Facilities Today
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	**Tallahassee, FL**	**Suspected ransomware forces Tallahassee hospital to divert EMS** The 772-bed hospital took its IT systems offline, diverted EMS patients and accepted only local Level 1 traumas. All non-emergency surgeries and outpatient procedures were canceled.	**772-bed hospital** 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
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

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
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** CRITICAL	**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** CRITICAL	**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** CRITICAL	**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
Jan 2022	**New Mexico** CRITICAL	**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

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
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
Oct 2020	**Alaska** CRITICAL	**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** CRITICAL	**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

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
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** CRITICAL	**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
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** CRITICAL	**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

DATE	JURISDICTION	WHAT HAPPENED	SCALE · SOURCE
Sep 2017	**Wisconsin** CRITICAL	**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** CRITICAL	**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** CRITICAL	**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)
Jun 2016	**Illinois** CRITICAL	**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** CRITICAL	**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** CRITICAL	**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** CRITICAL	**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** CRITICAL	**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** CRITICAL	**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

JURISDICTION PROFILES · 50 STATES + D.C.

Every state, on one page

2025 FBI cybercrime figures, confirmed ransomware attacks, and every documented incident in each jurisdiction.

Alabama AL · South

#46 of 51

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

Jul 2026 Iran-linked campaign hits Childersburg utility control network. Security Affairs

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

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

Alaska AK · West

#2 of 51

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

Sep 2025 Anchorage health center takes systems offline after breach. Becker's Hospital Review

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

Arizona AZ · West

#4 of 51

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

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

Oct 2023 Cyberattack disrupts Safford hospital's communication systems. The Record

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

Arkansas AR · South

#45 of 51

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

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

Mar 2025 EHR vendor breach exposes Arkansas Heart Hospital patient records. ClaimDepot

Nov 2022 Vendor cyberattack takes Arkansas county offices offline. KY3

California CA · West

#13 of 51

116,414	296	$3.67B
COMPLAINTS	PER 100K	LOSSES

Nov 2023 Cyberattack forces Oceanside hospital to divert ambulances. Becker's Hospital Review

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

Colorado CO · West

#7 of 51

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

Nov 2026 NEW Colorado election results website down about 45 minutes on election night. Colorado Politics

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

May 2024 Delta Health cyberattack exposes data of 148,363 people. DataBreaches.net

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

Connecticut CT · Northeast

#25 of 51

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

Jan 2026 Cyberattack disrupts New Britain municipal systems. Connecticut Public

Aug 2023 Prospect Medical attack closes two Connecticut ERs. Connecticut Public

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

Delaware DE · South

#15 of 51

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

- Sep 2024 Ransomware disrupts Delaware public libraries statewide. The Register
- Jul 2024 Rhysida ransomware gang breaches Bayhealth, 497,000 affected. GovInfoSecurity
- 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
COMPLAINTS	PER 100K	LOSSES

- Oct 2026 NEW FEC takes e-filing system offline after reported hacking attempt. eSecurity Planet
- Jun 2026 Cyberattack compromises D.C. Housing Authority systems, website down. WJLA 7News
- Jul 2025 SharePoint zero-day used to breach U.S. nuclear weapons agency. BleepingComputer
- Oct 2023 D.C. voter data stolen through a vendor server. The Record

Florida FL · South

#11 of 51

71,843	306	$1.60B
COMPLAINTS	PER 100K	LOSSES

- Oct 2026 NEW Florida student aid website breach may affect 4.9 million people. WWSB ABC7
- Jul 2024 RansomHub leaks data stolen from Florida health department. GovInfoSecurity
- Feb 2023 Suspected ransomware forces Tallahassee hospital to divert EMS. The Record
- 2016 Russian-linked hackers accessed voter data in two Florida counties. WFSU

Georgia GA · South

#35 of 51

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

- Nov 2024 Embargo ransomware knocks out Bainbridge hospital's health records. The Record
- Oct 2024 State repels attempt to crash absentee ballot request portal. Atlanta News First
- Jan 2024 Fulton County, Ga., systems taken down. SecurityWeek

Hawaii HI · West

#32 of 51

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

- Aug 2025 Ransomware hits UH Cancer Center, research data of 1.2M exposed. HIPAA Journal
- May 2024 Alleged LockBit attack shuts Maui health center two weeks. Hawaii News Now
- Jan 2023 Stolen login used to access Hawaii death registry records. The Record

Idaho ID · West

#40 of 51

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

- Oct 2026 NEW Ransomware attack closes Jerome School District for two days. Government Technology
- Mar 2026 Ransomware attack on Kootenai County exposes resident data. Coeur d'Alene Press
- May 2023 Cyberattack diverts ambulances from Idaho Falls hospital. The Record
- May 2018 Hackers deface Idaho Legislature and iCourt websites. KIVI-TV

Illinois IL · Midwest

#26 of 51

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

- Sep 2025 IDHS maps exposed data on ~700,000 residents for years. BleepingComputer
- Feb 2024 Rhysida ransomware takes Lurie Children's network offline. The Record
- Jun 2016 Illinois voter registration database breached. CBS Chicago

Indiana IN · Midwest

#12 of 51

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

- Jul 2024 Ransomware closes Clay County courthouse; disaster declared. The Record
- Apr 2024 Russia-linked hacktivists target Tipton wastewater plant. The Record
- Nov 2016 Ransomware halts online posting of county election results. Meridian Star (AP)

Iowa IA · Midwest · Priority

#51 of 51

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

Jan 2024 Ransomware hits Muscatine power and water utility. The Record

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

Kansas KS · Midwest · Priority

#22 of 51

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

Sep 2024 Cyberattack forces Kansas water plant to manual operations. SecurityWeek

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

Oct 2023 Kansas court system hit by foreign cyberattack. WIBW

Kentucky KY · South

#43 of 51

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

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

May 2023 BlackCat ransomware forces Norton hospitals onto paper records. The Record

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
COMPLAINTS	PER 100K	LOSSES

Oct 2026 NEW Database error wrongly marks 67,000 Louisiana voters inactive. The Center Square / Just The News

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)

Maine ME · Northeast

#44 of 51

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

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

Jun 2025 Cyber incidents at Lewiston hospitals force ambulance diversions. EMS1 / Morning Sentinel

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

Maryland MD · South

#8 of 51

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

Oct 2026 NEW Anne Arundel County confirms breach as Rhysida demands $2 million. The Record

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

Jan 2025 Ransomware forces Frederick Health to divert ambulances. Daily Security Review

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

Massachusetts MA · Northeast

#5 of 51

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

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

Nov 2023 Chinese Volt Typhoon hackers lurked in Littleton utility 300 days. The Record

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

Michigan MI · Midwest

#41 of 51

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

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

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

Aug 2024 Cyberattack on McLaren diverts ambulances, postpones care. Chief Healthcare Executive

Minnesota MN · Midwest

#31 of 51

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

- **Jul 2025** Cyberattack on St. Paul prompts National Guard activation. KTTC
- **Feb 2024** Attack on radiology firm disrupts reads for 22 hospitals. AuntMinnie
- **Feb 2023** Medusa leaks Minneapolis schools data after $1M demand. The Record

Mississippi MS · South

#50 of 51

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

- **Oct 2026** NEW Ransomware forces Vicksburg to shut down city systems. The Record
- **Oct 2026** NEW Attack on web provider disrupts about 70 Mississippi government websites. WLOX
- **Aug 2023** Ransomware takes Singing River hospitals offline, slows labs. Chief Healthcare Executive
- **Nov 2022** Election Day DDoS knocks Secretary of State sites offline. Mississippi Secretary of State

Missouri MO · Midwest

#38 of 51

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

- **Apr 2024** Ransomware hits Jackson County on election day. KCTV5
- **Oct 2023** Cyberattack cuts St. Louis paratransit to dialysis trips only. The Record
- **Jun 2023** MOVEit breach via IBM exposes Missouri Medicaid data. The Record

Montana MT · West

#36 of 51

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

- **Aug 2024** Meow ransomware gang claims attack on Anaconda critical access hospital. Comparitech
- **Apr 2023** Cyberattack on MSU brings in Montana National Guard. NBC Montana
- **Sep 2017** School network hack closes 30+ Flathead Valley schools. CBS News

Nebraska NE · Midwest · Priority

#48 of 51

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

- **Oct 2026** NEW North Platte and Lincoln County, Neb., knocked offline. Government Technology
- **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
COMPLAINTS	PER 100K	LOSSES

- **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)

New Hampshire NH · Northeast

#9 of 51

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

- **May 2025** Cyberattack forces Covenant Health offline, hitting Nashua hospital services. The Record
- **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

New Jersey NJ · Northeast

#42 of 51

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

- **Mar 2026** Malware attack knocks out Passaic County phones and IT. The Record
- **Oct 2024** Hackers breach largest U.S. water utility; billing and portal shut down. NJBIZ
- **May 2022** Ransomware hits Somerset County weeks before NJ primary. StateScoop

New Mexico NM · West

#21 of 51

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

Oct 2026 NEW Cyberattack diverts ambulances from University of New Mexico Hospital. Help Net Security

Mar 2024 Ransomware locks prosecutors out of files statewide. Government Technology

Jan 2022 Ransomware halts Bernalillo County voter registration, jail locks. TechTarget

New York NY · Northeast

#37 of 51

45,255	226	$1.23B
COMPLAINTS	PER 100K	LOSSES

Oct 2026 NEW Ransomware cancels classes in Oneonta City School District. Cybernews

Oct 2023 Cyber threat forces three Hudson Valley facilities to divert ambulances. The Record

Sep 2022 BlackCat ransomware cripples Suffolk County government. The Record

Oct 2020 Ransomware days before election puts absentee requests at risk. WSKG

North Carolina NC · South

#34 of 51

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

Jan 2025 Cyberattack shuts Pinehurst radiology practice for over a month. HIPAA Journal

Nov 2023 Cyberattack leaves Bladen County operating at limited capacity. The Record

Dec 2017 LockCrypt ransomware hits Mecklenburg County; ransom refused. NACo County News

North Dakota ND · Midwest

#49 of 51

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

2026 Ransomware hits Minot water treatment plant server. KFYR-TV

Apr 2020 Maze ransomware hits fiber provider for ND state network. StateScoop

Ohio OH · Midwest

#33 of 51

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

May 2025 Interlock ransomware knocks Kettering Health's 14 hospitals offline. The Record

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

Oklahoma OK · South

#16 of 51

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

Nov 2026 NEW Technical issues delay results reporting in two Oklahoma counties. Oklahoma State Election Board

Dec 2025 Unauthorized access to taxpayer data in OkTAP portal. Oklahoma OMES (official notice)

Nov 2023 Ransomware forces Tulsa-area Hillcrest hospitals to divert ER patients. KGOU

May 2021 Tulsa ransomware shuts city services, leaks 18,000 files. Route Fifty

Oregon OR · West

#14 of 51

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

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
COMPLAINTS	PER 100K	LOSSES

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

Nov 2023 Iran-backed Cyber Av3ngers seize control of Aliquippa water booster station. CBS News Pittsburgh

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

Rhode Island RI · Northeast

#28 of 51

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

- 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
- Aug 2023 Prospect Medical cyberattack hits two Rhode Island hospitals. NewsRadio WPRO

South Carolina SC · South

#23 of 51

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

- Nov 2026 NEW SCVotes voter lookup tools fail intermittently on Election Day. WCSC Live 5 News
- Oct 2026 NEW Columbia, S.C. confirms ransomware attack disrupting online services. ABC News 4
- Jul 2026 Malware takes AnMed hospital network to paper charts. FOX Carolina
- 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)

South Dakota SD · Midwest · Priority

#20 of 51

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

- Aug 2026 Cyberattack hits part of Mitchell city computer network. Dakota News Now
- Jul 2026 Hackers target Rapid City wastewater lift station. Newsweek
- Jul 2026 Pennington County, S.D., systems knocked out. South Dakota Searchlight

Tennessee TN · South

#39 of 51

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

- May 2024 Ascension ransomware puts Saint Thomas ERs on ambulance diversion. WPLN
- 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)

Texas TX · South

#10 of 51

97,912	309	$1.83B
COMPLAINTS	PER 100K	LOSSES

- Oct 2026 NEW Software glitch backlogs nearly 600,000 Texas voter registrations. Political Wire
- Jan 2024 Russia-linked hackers cause Muleshoe water system to overflow. Fortune
- 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

Utah UT · West

#18 of 51

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

- Aug 2025 Interlock ransomware steals Box Elder County data, 81,664 notified. Comparitech
- Dec 2024 Ransomware hits network controlling Salt Lake City airport systems. KSL
- Jul 2020 University of Utah pays $457,000 after ransomware attack. BleepingComputer

Vermont VT · Northeast

#27 of 51

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

- Oct 2026 NEW Slate Valley school district refuses ransom after data breach. WCAX
- Jan 2025 Ransomware locks Addison Northwest schools out of servers. Addison Independent
- Mar 2017 Joblink breach puts unemployment filers' SSNs at risk. Vermont Public

Virginia VA · South

#17 of 51

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

- Oct 2026 NEW Richmond Public Schools offline for over a week after cyber incident. WTVR CBS 6
- 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

Washington WA · West

#6 of 51

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

Nov 2026 NEW Washington Secretary of State website hit by cyberattack. KOMO News

Feb 2025 Intruders take down Whitman Hospital's internal systems. DataBreaches.net

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	238	$92.6M
COMPLAINTS	PER 100K	LOSSES

Jan 2024 Cyberattack disrupts Beckley city computer network. The Record

Mar 2023 D#nut ransomware hits Montgomery General, EHR pulled offline. Healthcare Facilities Today

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

Wisconsin WI · Midwest

#19 of 51

16,680	279	$194.2M
COMPLAINTS	PER 100K	LOSSES

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

May 2024 Ascension cyberattack slows care at Milwaukee hospitals. PBS Wisconsin

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

Wyoming WY · West · Priority

#24 of 51

1,552	264	$25.8M
COMPLAINTS	PER 100K	LOSSES

Sep 2026 NEW 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

ENGAGEMENT PLAN

From exposure scan to self-healing systems

Start outside the fence, prove the controls, then harden every system.

PHASE 1 · 30 DAYS

Outside-in scan

- Public exposure and leaked-credential scan, no system access.
- Known exploited vulnerability list matched to the asset inventory.
- Priority list for water, health and election networks.

PHASE 2 · 2027

Pilot the stack

- Self-scan and self-heal on one agency's services.
- LATCHKEY keys for every privileged account.
- First timed restore drill and incident exercise.

PHASE 3 · 2027 – 2028

Scale

- PATCH ROLL and CIS hardening statewide.
- OT isolation for water and utility controls.
- Same receipts and drills in every state.

BB2G
BORN BETWEEN 2 GENERALS

Decision requested

Authorize an outside-in exposure scan to set owners, priorities and success measures for a cyber readiness pilot.

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. Comparitech, confirmed ransomware attacks on U.S. organizations by state, 2018 – June 2022
4. CISA, Known Exploited Vulnerabilities Catalog
5. CISA, Secure by Design
6. NIST SP 800-218, Secure Software Development Framework
7. **US** Center for Internet Security, “CIS Election Day summary: probing, password guessing, DDoS-style traffic” (Nov 2026)
8. **US** Nextgov/FCW, “Election offices report failed hacking attempts on Election Day” (Nov 2026)
9. **US** Help Net Security, “FBI warns of midterm scams including fake voter registration pages” (Oct 2026)
10. **US** CyberScoop, “Cyber incident at contractor halts federal bankruptcy notices nationwide” (Oct 2026)
11. **AL** Alabama Political Reporter, “DDoS attacks slow Alabama state government websites” (Mar 2024)
12. **AL** Government Technology, “State IT office investigates breach affecting state systems” (May 2025)
13. **AL** Security Affairs, “Iran-linked campaign hits Childersburg utility control network” (Jul 2026)
14. **AK** Alaska Public Media, “Hackers steal Alaska voter data from online registration system” (Oct 2020)
15. **AK** The Record, “Nation-state attackers breach Alaska health department network” (May 2021)
16. **AK** Becker's Hospital Review, “Anchorage health center takes systems offline after breach” (Sep 2025)
17. **AZ** CBS News, “Malware attempt via Gila County targets Arizona voter database” (2016)
18. **AZ** The Record, “Cyberattack disrupts Safford hospital's communication systems” (Oct 2023)
19. **AZ** Votebeat, “Attackers breach Arizona election candidate portal, post Khomeini image” (Jun 2025)
20. **AR** KY3, “Vendor cyberattack takes Arkansas county offices offline” (Nov 2022)
21. **AR** ClaimDepot, “EHR vendor breach exposes Arkansas Heart Hospital patient records” (Mar 2025)
22. **AR** Talk Business & Politics, “Cyberattack knocks out Fort Smith schools' phones and internet” (Jul 2025)
23. **CA** KQED, “Riverside DA: hackers altered voters' party registrations in 2016” (Jun 2016)
24. **CA** KPBS (AP), “MOVEit breach exposes data of 769,000 CalPERS retirees” (Jun 2023)
25. **CA** Becker's Hospital Review, “Cyberattack forces Oceanside hospital to divert ambulances” (Nov 2023)
26. **CO** SecurityWeek, “MOVEit breach exposes data of 4 million Colorado Medicaid members” (May 2023)
27. **CO** DataBreaches.net, “Delta Health cyberattack exposes data of 148,363 people” (May 2024)
28. **CO** Colorado Public Radio, “Voting equipment BIOS passwords left exposed on state website” (Oct 2024)
29. **CO** Colorado Politics, “Colorado election results website down about 45 minutes on election night” (Nov 2026)
30. **CT** Connecticut Secretary of the State, “Russian agents targeted Connecticut voter registration system” (2016)

31. **CT** Connecticut Public, “Prospect Medical attack closes two Connecticut ERs” (Aug 2023)
32. **CT** Connecticut Public, “Cyberattack disrupts New Britain municipal systems” (Jan 2026)
33. **DE** Delaware Public Media, “Russian hackers attempted to access Delaware voter registration” (2016)
34. **DE** GovInfoSecurity, “Rhysida ransomware gang breaches Bayhealth, 497,000 affected” (Jul 2024)
35. **DE** The Register, “Ransomware disrupts Delaware public libraries statewide” (Sep 2024)
36. **DC** The Record, “D.C. voter data stolen through a vendor server” (Oct 2023)
37. **DC** BleepingComputer, “SharePoint zero-day used to breach U.S. nuclear weapons agency” (Jul 2025)
38. **DC** WJLA 7News, “Cyberattack compromises D.C. Housing Authority systems, website down” (Jun 2026)
39. **DC** eSecurity Planet, “FEC takes e-filing system offline after reported hacking attempt” (Oct 2026)
40. **FL** WFSU, “Russian-linked hackers accessed voter data in two Florida counties” (2016)
41. **FL** The Record, “Suspected ransomware forces Tallahassee hospital to divert EMS” (Feb 2023)
42. **FL** GovInfoSecurity, “RansomHub leaks data stolen from Florida health department” (Jul 2024)
43. **FL** WWSB ABC7, “Florida student aid website breach may affect 4.9 million people” (Oct 2026)
44. **GA** SecurityWeek, “Fulton County, Ga., systems taken down” (Jan 2024)
45. **GA** Atlanta News First, “State repels attempt to crash absentee ballot request portal” (Oct 2024)
46. **GA** The Record, “Embargo ransomware knocks out Bainbridge hospital's health records” (Nov 2024)
47. **HI** The Record, “Stolen login used to access Hawaii death registry records” (Jan 2023)
48. **HI** Hawaii News Now, “Alleged LockBit attack shuts Maui health center two weeks” (May 2024)
49. **HI** HIPAA Journal, “Ransomware hits UH Cancer Center, research data of 1.2M exposed” (Aug 2025)
50. **ID** KIVI-TV, “Hackers deface Idaho Legislature and iCourt websites” (May 2018)
51. **ID** The Record, “Cyberattack diverts ambulances from Idaho Falls hospital” (May 2023)
52. **ID** Coeur d'Alene Press, “Ransomware attack on Kootenai County exposes resident data” (Mar 2026)
53. **ID** Government Technology, “Ransomware attack closes Jerome School District for two days” (Oct 2026)
54. **IL** CBS Chicago, “Illinois voter registration database breached” (Jun 2016)
55. **IL** The Record, “Rhysida ransomware takes Lurie Children's network offline” (Feb 2024)
56. **IL** BleepingComputer, “IDHS maps exposed data on ~700,000 residents for years” (Sep 2025)
57. **IN** Meridian Star (AP), “Ransomware halts online posting of county election results” (Nov 2016)
58. **IN** The Record, “Russia-linked hacktivists target Tipton wastewater plant” (Apr 2024)
59. **IN** The Record, “Ransomware closes Clay County courthouse; disaster declared” (Jul 2024)
60. **IA** Iowa Capital Dispatch, “Hack at records vendor cuts Iowa counties off from land records” (Dec 2022)
61. **IA** District Administration, “Des Moines Public Schools hit by ransomware” (Jan 2023)
62. **IA** The Record, “Ransomware hits Muscatine power and water utility” (Jan 2024)
63. **KS** WIBW, “Kansas court system hit by foreign cyberattack” (Oct 2023)
64. **KS** Insurance Journal, “Ransomware attackers steal personal, medical data from Franklin County” (May 2024)
65. **KS** SecurityWeek, “Cyberattack forces Kansas water plant to manual operations” (Sep 2024)
66. **KY** Louisville Public Media, “Pro-Russian DDoS knocks Kentucky elections and courts sites offline” (Oct 2022)
67. **KY** The Record, “BlackCat ransomware forces Norton hospitals onto paper records” (May 2023)
68. **KY** Comparitech, “Ransomware shuts Jefferson County Clerk's offices for a week” (Jul 2024)
69. **LA** Insurance Journal (AP), “Attempted ransomware attack disrupts nearly every state agency” (Nov 2019)
70. **LA** WAFB, “MOVEit breach exposes records of nearly every Louisiana driver” (Jun 2023)
71. **LA** The Center Square / Just The News, “Database error wrongly marks 67,000 Louisiana voters inactive” (Oct 2026)
72. **ME** Cybersecurity Dive, “MOVEit breach hits roughly the entire population of Maine” (May 2023)
73. **ME** EMS1 / Morning Sentinel, “Cyber incidents at Lewiston hospitals force ambulance diversions” (Jun 2025)
74. **ME** Bangor Daily News, “Cyberattack forces Bar Harbor offline, water plant controls cut” (Jul 2025)
75. **MD** NBC Washington (AP), “RobbinHood ransomware cripples Baltimore city network” (May 2019)
76. **MD** Daily Security Review, “Ransomware forces Frederick Health to divert ambulances” (Jan 2025)
77. **MD** The Daily Record, “Cyberattack disrupts Maryland transit systems, data lost” (Aug 2025)
78. **MD** The Record, “Anne Arundel County confirms breach as Rhysida demands $2 million” (Oct 2026)
79. **MA** SecurityWeek, “Ransomware hits state ferry agency, delaying ticketing” (Jun 2021)
80. **MA** The Record, “Chinese Volt Typhoon hackers lurked in Littleton utility 300 days” (Nov 2023)
81. **MA** WJAR (NBC 10), “Attleboro intrusion may have exposed SSNs and medical data” (Nov 2025)
82. **MI** Chief Healthcare Executive, “Cyberattack on McLaren diverts ambulances, postpones care” (Aug 2024)
83. **MI** The Record, “Cyberattack takes Michigan's largest county offline” (Oct 2024)
84. **MI** Comparitech, “Ransomware gang hits Michigan county on Election Day” (Nov 2024)
85. **MN** The Record, “Medusa leaks Minneapolis schools data after $1M demand” (Feb 2023)
86. **MN** AuntMinnie, “Attack on radiology firm disrupts reads for 22 hospitals” (Feb 2024)
87. **MN** KTTC, “Cyberattack on St. Paul prompts National Guard activation” (Jul 2025)
88. **MS** Mississippi Secretary of State, “Election Day DDoS knocks Secretary of State sites offline” (Nov 2022)
89. **MS** Chief Healthcare Executive, “Ransomware takes Singing River hospitals offline, slows labs” (Aug 2023)
90. **MS** The Record, “Ransomware forces Vicksburg to shut down city systems” (Oct 2026)
91. **MS** WLOX, “Attack on web provider disrupts about 70 Mississippi government websites” (Oct 2026)
92. **MO** The Record, “MOVEit breach via IBM exposes Missouri Medicaid data” (Jun 2023)
93. **MO** The Record, “Cyberattack cuts St. Louis paratransit to dialysis trips only” (Oct 2023)
94. **MO** KCTV5, “Ransomware hits Jackson County on election day” (Apr 2024)
95. **MT** CBS News, “School network hack closes 30+ Flathead Valley schools” (Sep 2017)
96. **MT** NBC Montana, “Cyberattack on MSU brings in Montana National Guard” (Apr 2023)
97. **MT** Comparitech, “Meow ransomware gang claims attack on Anaconda critical access hospital” (Aug 2024)
98. **NE** Nebraska Examiner, “Change Healthcare ransomware reaches 575,000+ Nebraskans” (Feb 2024)
99. **NE** Nebraska Attorney General, “Nebraska bank network intrusion” (Jan 2025)

100. **NE** Government Technology, “North Platte and Lincoln County, Neb., knocked offline” (Oct 2026)
101. **NV** News 3 Las Vegas (KSNV), “Unauthorized party breaches Clark County schools email system” (Oct 2023)
102. **NV** ABC News, “Nevada state offices shut by cyberattack” (Aug 2025)
103. **NH** New Hampshire Public Radio, “Email fraud diverts $2.3M in Peterborough town funds” (Aug 2021)
104. **NH** Associated Press (via Boston.com), “AI-generated 'Biden' robocall urges NH voters to skip primary” (Jan 2024)
105. **NH** The Record, “Cyberattack forces Covenant Health offline, hitting Nashua hospital services” (May 2025)
106. **NJ** StateScoop, “Ransomware hits Somerset County weeks before NJ primary” (May 2022)
107. **NJ** NJBIZ, “Hackers breach largest U.S. water utility; billing and portal shut down” (Oct 2024)
108. **NJ** The Record, “Malware attack knocks out Passaic County phones and IT” (Mar 2026)
109. **NM** TechTarget, “Ransomware halts Bernalillo County voter registration, jail locks” (Jan 2022)
110. **NM** Government Technology, “Ransomware locks prosecutors out of files statewide” (Mar 2024)
111. **NM** Help Net Security, “Cyberattack diverts ambulances from University of New Mexico Hospital” (Oct 2026)
112. **NY** WSKG, “Ransomware days before election puts absentee requests at risk” (Oct 2020)
113. **NY** The Record, “BlackCat ransomware cripples Suffolk County government” (Sep 2022)
114. **NY** The Record, “Cyber threat forces three Hudson Valley facilities to divert ambulances” (Oct 2023)
115. **NY** Cybernews, “Ransomware cancels classes in Oneonta City School District” (Oct 2026)
116. **NC** NACo County News, “LockCrypt ransomware hits Mecklenburg County; ransom refused” (Dec 2017)
117. **NC** The Record, “Cyberattack leaves Bladen County operating at limited capacity” (Nov 2023)
118. **NC** HIPAA Journal, “Cyberattack shuts Pinehurst radiology practice for over a month” (Jan 2025)
119. **ND** StateScoop, “Maze ransomware hits fiber provider for ND state network” (Apr 2020)
120. **ND** KFYR-TV, “Ransomware hits Minot water treatment plant server” (2026)
121. **OH** WCBE, “Attackers try to inject code into Ohio SOS website” (Nov 2019)
122. **OH** Infosecurity Magazine, “Rhysida ransomware exposes data of 500,000 Columbus residents” (Jul 2024)
123. **OH** The Record, “Interlock ransomware knocks Kettering Health's 14 hospitals offline” (May 2025)
124. **OK** Route Fifty, “Tulsa ransomware shuts city services, leaks 18,000 files” (May 2021)
125. **OK** KGOU, “Ransomware forces Tulsa-area Hillcrest hospitals to divert ER patients” (Nov 2023)
126. **OK** Oklahoma OMES (official notice), “Unauthorized access to taxpayer data in OkTAP portal” (Dec 2025)
127. **OK** Oklahoma State Election Board, “Technical issues delay results reporting in two Oklahoma counties” (Nov 2026)
128. **OR** BleepingComputer, “Phishing exposes data of 645,000 Oregon DHS clients” (Jan 2019)
129. **OR** Oregon DOT (official notice), “MOVEit hack exposes 3.5M Oregon driver's license records” (Jun 2023)
130. **PA** 6abc Philadelphia, “Ransomware encrypts Delaware County police and payroll data” (Nov 2020)
131. **PA** CBS News Pittsburgh, “Iran-backed Cyber Av3ngers seize control of Aliquippa water booster station” (Nov 2023)
132. **PA** Infosecurity Magazine, “Ransomware takes PA Attorney General's office offline” (Aug 2025)
133. **RI** NewsRadio WPRO, “Prospect Medical cyberattack hits two Rhode Island hospitals” (Aug 2023)
134. **RI** Rhode Island Current, “Medusa ransomware hits Providence schools, demands $1M” (Sep 2024)
135. **RI** Rhode Island Current, “Brain Cipher breach of RIBridges benefits system exposes 644,000 people” (Dec 2024)
136. **SC** GovTech (via The State), “Nearly 150,000 attempts to penetrate S.C. voter registration system” (Nov 2016)
137. **SC** The Record, “Ransomware attack disrupts Spartanburg County IT and phone systems” (Apr 2023)
138. **SC** FOX Carolina, “Malware takes AnMed hospital network to paper charts” (Jul 2026)
139. **SC** ABC News 4, “Columbia, S.C. confirms ransomware attack disrupting online services” (Oct 2026)
140. **SC** WCSC Live 5 News, “SCVotes voter lookup tools fail intermittently on Election Day” (Nov 2026)
141. **SD** Newsweek, “Hackers target Rapid City wastewater lift station” (Jul 2026)
142. **SD** South Dakota Searchlight, “Pennington County, S.D., systems knocked out” (Jul 2026)
143. **SD** Dakota News Now, “Cyberattack hits part of Mitchell city computer network” (Aug 2026)
144. **TN** Phys.org (AP), “Election-night results website knocked offline in Knox County” (May 2018)
145. **TN** The Record, “Ransomware attack takes Oak Ridge city network offline” (Mar 2023)
146. **TN** WPLN, “Ascension ransomware puts Saint Thomas ERs on ambulance diversion” (May 2024)
147. **TX** KERA News, “Coordinated ransomware attack hits 23 Texas local governments” (Aug 2019)
148. **TX** Dallas Morning News, “Royal ransomware shuts Dallas courts, disrupts police systems” (May 2023)
149. **TX** Fortune, “Russia-linked hackers cause Muleshoe water system to overflow” (Jan 2024)
150. **TX** Political Wire, “Software glitch backlogs nearly 600,000 Texas voter registrations” (Oct 2026)
151. **UT** BleepingComputer, “University of Utah pays $457,000 after ransomware attack” (Jul 2020)
152. **UT** KSL, “Ransomware hits network controlling Salt Lake City airport systems” (Dec 2024)
153. **UT** Comparitech, “Interlock ransomware steals Box Elder County data, 81,664 notified” (Aug 2025)
154. **VT** Vermont Public, “Joblink breach puts unemployment filers' SSNs at risk” (Mar 2017)
155. **VT** Addison Independent, “Ransomware locks Addison Northwest schools out of servers” (Jan 2025)
156. **VT** WCAX, “Slate Valley school district refuses ransom after data breach” (Oct 2026)
157. **VA** UPI, “Ransomware hits Virginia legislature's IT agency, websites” (Dec 2021)
158. **VA** Insurance Journal (Washington Post), “Cyberattack forces Virginia attorney general's office offline” (Feb 2025)
159. **VA** WTVR CBS 6, “Richmond Public Schools offline for over a week after cyber incident” (Oct 2026)
160. **WA** Northwest Public Broadcasting, “Accellion breach may expose 1.6M Washington jobless claims” (Feb 2021)
161. **WA** SecurityWeek, “Rhysida ransomware disrupts Sea-Tac and exposes 90,000 people” (Aug 2024)
162. **WA** DataBreaches.net, “Intruders take down Whitman Hospital's internal systems” (Feb 2025)
163. **WA** KOMO News, “Washington Secretary of State website hit by cyberattack” (Nov 2026)
164. **WV** The Record, “Cyberattack cancels classes for 20,000 Berkeley County students” (Feb 2023)

165. **WV** Healthcare Facilities Today, “D#nut ransomware hits Montgomery General, EHR pulled offline” (Mar 2023)
166. **WV** The Record, “Cyberattack disrupts Beckley city computer network” (Jan 2024)
167. **WI** WPR, “DHS confirms Russian hackers targeted Wisconsin in 2016” (Sep 2017)
168. **WI** PBS Wisconsin, “Ascension cyberattack slows care at Milwaukee hospitals” (May 2024)
169. **WI** The Record, “Chort ransomware steals data on 67,000 Sheboygan residents” (Oct 2024)
170. **WY** Wyoming Department of Health, “Wyoming health test data posted to public GitHub” (Apr 2021)
171. **WY** Wyoming Public Media, “Court vendor breach exposes Wyoming court users' personal data” (Sep 2026)