Major U.S. Data Breaches and Cyberattacks

Union of Saints

Who, What, When, Where, Why, How, Perpetrators, Government Connections, Arrests, Wanted Status, and Executive Accountability

Report date: October 23, 2026

Example:

The Equifax indictment specifically identified four alleged members of China's People's Liberation Army, while the Yahoo case involved two alleged Russian FSB officers working with criminal hackers. These are materially different types of operations and should be documented separately.



United States Department of Justice
+1

Purpose and scope

This report documents major data breaches and cyberattacks affecting U.S. government agencies, financial institutions, healthcare organizations, retailers, telecommunications companies, software providers, and social media platforms.

For every incident, the investigation should establish:

1. **Who:** The affected organization, named suspects, alleged accomplices, executives, and government agencies involved.
2. **What:** The information stolen, systems compromised, and approximate number of affected people.
3. **When:** When the attack began, when it was discovered, when it was disclosed, and when legal action occurred.
4. **Where:** The affected organization's location, the countries associated with the alleged perpetrators, and the countries where arrests or prosecutions occurred.
5. **Why:** The documented or alleged motive, such as financial theft, espionage, extortion, intelligence collection, or unauthorized data collection.
6. **How:** The technical or operational method used to gain access.

7. **Government connection:** Whether the suspect was a government employee, military member, intelligence officer, state contractor, alleged state-sponsored hacker, or apparently independent criminal.
8. **Arrests and wanted status:** Whether suspects were arrested, charged, convicted, sentenced, extradited, or listed as wanted, with the relevant date and source.
9. **Institutional accountability:** The CEO, agency director, CIO, CISO, and other relevant leaders at the time, alongside documented regulatory findings and corrective actions.

A country associated with a suspect is not necessarily the location from which an attack was launched. A government's attribution of a cyberattack is not equivalent to proof of an individual's guilt. All allegations must be distinguished from convictions, and historical wanted status must be distinguished from current status.

Part I. Government and national security incidents

1. U.S. Office of Personnel Management (OPM), 2014–2015

Who was affected: Federal employees, former employees, contractors, and people who underwent federal background investigations.

What happened: Intruders accessed personnel systems and stole sensitive personal information. The background investigation incident affected approximately 21.5 million people. A separate personnel records incident also occurred.

When: Related activity was identified in 2014 and 2015. The major background investigation breach was discovered in May 2015 and disclosed in June 2015.

Where: U.S. federal government systems. U.S. officials attributed the operation to Chinese state-linked actors.

How: Unauthorized access to federal systems allowed the theft of extensive personnel and background investigation information.

Why: The exact motives of the individuals involved have not been established in a public criminal conviction directly tied to the breach. Intelligence collection is a significant concern because the records contained sensitive information about federal personnel and people with security clearances.

Perpetrators and government connection: U.S. authorities attributed the operation to Chinese state-linked actors. Publicly established information summarized here does not identify a confirmed individual perpetrator who was prosecuted directly for the OPM breach.

Arrests and wanted status: No publicly announced arrest directly tied to the OPM breach has been verified in this report. This should not be interpreted as proof that no investigation or intelligence attribution exists.

Leadership: Katherine Archuleta was OPM Director. Donna Seymour was CIO during the incident period.

Accountability questions: What weaknesses in identity management, system monitoring, and access controls permitted the intrusion? What security deficiencies were known before the incident? What changes followed?

Sources: https://www.opm.gov/ and https://www.gao.gov/

2. Equifax, 2017

Who was affected: Approximately 145.5 million U.S. consumers in the initial reported total.

What happened: Attackers stole personal information, including names, birth dates, Social Security numbers, addresses, and other sensitive data.

When: The intrusion occurred from May through July 2017. Equifax discovered it on July 29 and disclosed it publicly on September 7.

Where: Equifax's U.S. systems. Investigators alleged that the attackers used servers in multiple countries to disguise the origin of their activity.

How: The attackers exploited a vulnerability in Apache Struts software used by Equifax's online dispute portal. According to the indictment, they obtained credentials, explored databases, collected sensitive information, and transferred the stolen data outside the network.

Why: The U.S. indictment alleged theft of personal information and trade secrets. The ultimate motives of each individual have not been established by a conviction in the cited case.

Named suspects: Wu Zhiyong, Wang Qian, Xu Ke, and Liu Lei.

Country and government connection: The U.S. Department of Justice alleged that all four were members of China's People's Liberation Army, specifically its 54th Research Institute. This is an alleged direct military connection, rather than merely an assertion that the hackers operated from China.

Arrests and wanted status: The four were indicted in the United States in February 2020. The cited announcement does not establish that they were arrested or convicted. The FBI maintains a wanted poster for the four individuals; current status should be checked against the live official notice.

Leadership: Richard F. Smith was chairman and CEO. He stepped down in September 2017.

Accountability questions: Why was the software vulnerability not addressed in time? What controls restricted database access? How effective were security monitoring and internal escalation procedures?

Sources:

- DOJ indictment announcement: https://www.justice.gov/archives/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking
- FBI wanted notice: https://www.fbi.gov/wanted/cyber/chinese-pla-members-54th-research-institute

3. SolarWinds, 2019–2020

Who was affected: U.S. government agencies and private-sector organizations using affected SolarWinds Orion software.

What happened: Malicious code was inserted into software updates and distributed to customers. The compromised updates provided attackers with opportunities to access selected customer networks.

When: The campaign began in 2019 and was publicly disclosed in December 2020.

Where: SolarWinds and customer networks in the United States and other countries. The U.S. government attributed the campaign to Russia's Foreign Intelligence Service.

How: Attackers compromised a trusted software distribution process, allowing malicious code to be delivered through legitimate updates.

Why: The operation was characterized by U.S. authorities as a state-sponsored intelligence campaign.

Named suspects: The public attribution summarized here identifies a Russian intelligence service rather than a fully prosecuted roster of individual perpetrators.

Country and government connection: Russia; attributed to a Russian foreign intelligence service. This is an alleged state intelligence operation, not simply a criminal attack originating from a Russian IP address.

Arrests and wanted status: This report does not establish a named individual arrest directly tied to the entire SolarWinds campaign. Individual legal developments must be verified separately.

Leadership: Kevin Thompson was CEO during much of the intrusion period. Sudhakar Ramakrishna became CEO in January 2021.

Accountability questions: How were software development and distribution systems protected? What monitoring could detect malicious updates? Which customers experienced actual follow-on compromise?

Sources: https://www.cisa.gov/ and https://www.justice.gov/news

4. Microsoft Exchange Server, 2021

Who was affected: Organizations operating vulnerable on-premises Microsoft Exchange servers around the world.

What happened: Attackers exploited vulnerabilities to access email systems and install persistent web shells.

When: The major exploitation campaign became public in 2021, although related allegations concern intrusions beginning in 2020.

Where: Worldwide, including the United States.

How: Attackers exploited vulnerabilities in internet-facing email servers to gain unauthorized access and maintain persistence.

Why: U.S. authorities have described activity associated with the broader campaign as state-directed espionage and intelligence collection.

Named suspects: Xu Zewei and Zhang Yu were charged in a separate U.S. case concerning alleged intrusions from February 2020 through June 2021, including activity associated with the HAFNIUM campaign.

Country and government connection: Both are Chinese nationals. The U.S. indictment alleged that officers of China's Ministry of State Security, specifically its Shanghai State Security Bureau, directed the activity. This is an alleged intelligence-service connection.

Arrests and wanted status: Xu Zewei was arrested in Milan, Italy, on July 3, 2025, at the request of the United States, and faced extradition proceedings at the time of the DOJ announcement. Zhang Yu was charged; this report does not establish his current arrest or wanted status.

Leadership: Satya Nadella was Microsoft CEO.

Sources:

- DOJ announcement: https://www.justice.gov/opa/pr/justice-department-announces-arrest-prolific-chinese-state-sponsored-contract-hacker
- CISA: https://www.cisa.gov/

Part II. Financial and retail incidents

5. TJX Companies, 2005–2007

What happened: Payment card information was stolen from retail systems, making this one of the major early retail payment card hacking cases.

How: Attackers compromised payment processing systems and stole card data.

Named suspects and country: Albert Gonzalez, a U.S. national, was a central defendant in the broader payment card hacking investigations. The broader conspiracy involved additional participants; each person's role must be established from court records.

Government connection: No government direction has been established in the cited case summary. The incident is generally treated as criminal financial hacking.

Arrests and legal outcome: Gonzalez was prosecuted and pleaded guilty in the broader payment card cases. Exact case-specific charges and sentencing records should be consulted.

Leadership: Executive tenure and security leadership should be verified against company filings from the relevant dates.

Sources: https://www.justice.gov/news

6. Heartland Payment Systems, 2008–2009

What happened: Approximately 130 million payment card numbers were reported compromised.

How: Attackers penetrated a payment processor and stole payment card data.

Named suspect: Albert Gonzalez was prosecuted in the broader payment card hacking cases.

Country and government connection: Gonzalez was a U.S. national. The case is documented as criminal hacking and financial theft, with no government-directed operation established in the cited summary.

Arrests and legal outcome: Gonzalez pleaded guilty in the broader case. The final report should cite the relevant charging and sentencing records.

Leadership: Heartland's executive and security leadership during the incident should be established through contemporaneous company records.

Sources: https://www.justice.gov/news

7. Target, 2013

What happened: Approximately 40 million payment card accounts were affected, with personal information associated with up to 70 million customers also exposed.

How: Attackers obtained access to Target's systems and compromised payment data during the holiday shopping season.

Named suspects and country: The breach was associated with criminal payment card activity, but this report does not establish a complete, court-verified list of named perpetrators directly responsible for the Target intrusion.

Government connection: No government-directed operation has been established in the cited summary.

Arrests and wanted status: A complete Target-specific list of arrests, charges, and convictions requires review of the relevant federal and state court records.

Leadership: Gregg Steinhafel was CEO and resigned in May 2014.

Accountability questions: How were credentials obtained? How was access to point-of-sale systems controlled? How quickly did monitoring identify suspicious activity?

Sources: https://www.ftc.gov/ and https://www.congress.gov/

8. Adobe, 2013

What happened: Approximately 153 million accounts were reported in breach databases. Exposed information included email addresses, usernames, encrypted passwords, and password hints.

How: Attackers accessed Adobe's systems and obtained account-related data.

Named suspects and country: A complete, verified roster of individual perpetrators and their countries is not established in the sources summarized here.

Government connection: No government-directed operation has been established in this report.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: Shantanu Narayen was CEO.

Accountability questions: How were passwords stored? What account recovery information was exposed? Did password reuse expose customers to additional attacks?

Sources: https://www.adobe.com/trust/security.html

9. eBay, 2014

What happened: Approximately 145 million users were potentially affected when attackers accessed customer information.

How: Attackers obtained employee credentials and used them to access a customer database.

Named suspects and country: A complete named perpetrator list and verified country information are not established in the sources summarized here.

Government connection: No government-directed operation has been established in this report.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: John Donahoe was CEO.

Accountability questions: How were employee credentials compromised? What controls limited database access? How long did the unauthorized access continue?

Sources: https://www.ebayinc.com/

10. JPMorgan Chase, 2014

What happened: Approximately 76 million households and 7 million small businesses were affected.

How: Attackers obtained access to internal systems and customer-related information.

Named suspects and country: The source set summarized here does not establish a complete roster of individuals responsible for this specific breach.

Government connection: No government-directed operation has been established in this report.

Arrests and wanted status: A specific arrest or wanted status is not verified here.

Leadership: Jamie Dimon was CEO.

Accountability questions: What vulnerabilities and access controls enabled the intrusion? What information was actually accessed? What monitoring and remediation followed?

Sources: https://www.jpmorganchase.com/

11. Capital One, 2019

What happened: Approximately 106 million people in the United States and Canada were affected.

How: An attacker accessed credit card application data through a cloud infrastructure security vulnerability.

Named suspect: Paige Thompson.

Country and government connection: Thompson was a U.S. national. The case was prosecuted as criminal computer intrusion, not as a government-directed intelligence operation.

Arrest and legal outcome: Thompson was arrested and prosecuted. The final report should distinguish the arrest, verdict, and sentence using court records.

Leadership: Richard Fairbank was CEO.

Accountability questions: What cloud configuration or access controls failed? How was the incident detected? What information was accessible to the attacker?

Sources: https://www.justice.gov/news and https://www.capitalone.com/

Part III. Email and social media incidents

12. Yahoo, 2013–2014

What happened: Yahoo ultimately reported that all three billion accounts were affected by the 2013 incident. A separate 2014 intrusion affected at least 500 million accounts.

How: Attackers stole account information and used unauthorized access to obtain email contents and other information.

Named suspects and countries:

- **Dmitry Dokuchaev:** Russian national and resident; alleged Russian Federal Security Service (FSB) officer.
- **Igor Sushchin:** Russian national and resident; alleged FSB officer.
- **Alexsey Belan:** Russian national and resident, born in Latvia; alleged criminal hacker.
- **Karim Baratov:** Canadian and Kazakh national and resident of Canada; criminal hacker.

Government connection: The U.S. indictment alleged that Dokuchaev and Sushchin were FSB officers who directed, facilitated, and paid criminal hackers. The case is an example of an alleged intelligence service working with criminal actors.

Arrests and wanted status: Baratov was arrested in Canada in March 2017. He pleaded guilty in November 2017 and was sentenced in 2018. Dokuchaev, Sushchin, and Belan were described as fugitives in the 2017 announcement. Belan was subject to an Interpol Red Notice at that time. Current wanted status requires fresh official verification.

Leadership: Marissa Mayer was CEO during the major public disclosures in 2016.

Sources:

- DOJ case record: https://www.justice.gov/usao-ndca/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and
- Case docket and outcomes: https://www.justice.gov/usao-ndca/us-v-dmitry-dokuchaev-et-al

13. Facebook and Cambridge Analytica, 2010s–2018

What happened: Data from tens of millions of users was collected through an application and subsequently used by Cambridge Analytica for profiling and political targeting.

How: A third-party app collected data through Facebook's platform permissions and obtained information associated with users and some of their friends.

Named people and countries: Aleksandr Kogan was the app developer. Alexander Nix led Cambridge Analytica. The relevant company and individual records should be used to verify nationality and residence rather than infer them from names.

Government connection: The documented proceedings concern data collection and use by private companies. The controversy should not be described as a state-sponsored hacking operation without separate evidence.

Arrests and wanted status: FTC civil proceedings and settlements are not equivalent to criminal arrests or convictions. No specific arrest directly tied to this data collection is established in the sources summarized here.

Leadership: Mark Zuckerberg was CEO of Facebook.

Sources: https://www.ftc.gov/

14. LinkedIn, 2012 and 2016

What happened: Millions of password hashes were disclosed in 2012, and a much larger collection of account credentials surfaced in 2016.

How: Account credential data was obtained and subsequently circulated.

Named suspects and countries: A complete, verified list of perpetrators and countries of origin is not established here.

Government connection: No government-directed operation has been established in this report.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: Jeff Weiner was CEO.

Sources: https://news.linkedin.com/

15. Twitter, July 2020

What happened: Attackers took over approximately 130 targeted accounts, including those belonging to prominent public figures and companies.

How: Social engineering and unauthorized access to internal systems enabled account takeovers.

Named suspect: Joseph O'Connor.

Country and government connection: O'Connor was a British national. The case was treated as criminal hacking rather than a government-directed operation in the cited U.S. case summary.

Arrest and legal outcome: O'Connor was arrested in Spain in July 2021. Any current status or additional sentence information should be confirmed through official court records.

Leadership: Jack Dorsey was CEO.

Sources: https://www.justice.gov/news and https://www.fbi.gov/investigate/cyber

16. Facebook data scraping, disclosed in 2021

What happened: A dataset involving approximately 533 million users surfaced publicly in 2021.

How: The information had been collected through Facebook's contact-importer functionality before September 2019, according to Facebook's explanation.

Named suspects and countries: A complete, verified list of individuals responsible for the collection and public circulation is not established in the sources summarized here.

Government connection: No government-directed operation has been established in this report.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: Mark Zuckerberg was CEO.

Sources: https://about.fb.com/

17. 23andMe, 2023

What happened: Information associated with nearly seven million customers was affected through account compromise and the DNA Relatives feature.

How: Credential stuffing allowed attackers to access accounts, with additional information available through linked relationships and features.

Named suspects and countries: The sources summarized here do not establish a complete, court-verified list of individuals responsible for the overall incident.

Government connection: No government-directed operation has been established in this report.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: The relevant CEO and security leadership should be verified against company filings for the exact incident dates.

Sources: https://www.23andme.com/ and https://www.ftc.gov/

Part IV. Healthcare and health insurance

18. Anthem, 2015

What happened: Approximately 78.8 million people were affected by a breach involving health plan members and employees.

How: Attackers obtained unauthorized access to systems holding personal information.

Named suspects and countries: The sources summarized here do not establish a complete, individually prosecuted perpetrator list for the Anthem incident.

Government connection: The U.S. government publicly attributed the Equifax, OPM, Marriott, and Anthem incidents to Chinese state-linked activity in broader public statements.

Attribution of the Anthem incident should be cited to the specific original government assessment before naming individual perpetrators.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: Joseph Swedish was CEO.

Sources: https://www.justice.gov/news

19. Premera Blue Cross, 2014–2015

What happened: Approximately 11 million people were affected by a breach involving member and applicant information.

How: Attackers accessed systems holding health insurance-related data.

Named suspects and countries: A complete, verified list is not established in the sources summarized here.

Government connection: No specific individual government affiliation is established here.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: Jeff Roe was CEO during the disclosure period.

Sources: https://www.premera.com/

20. HCA Healthcare, 2023

What happened: Approximately 11.27 million people were affected by a data theft incident.

How: A threat actor reportedly stole and offered patient-related information for sale.

Named suspects and countries: The sources summarized here do not establish a complete verified list of named perpetrators or their government affiliations.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: Sam Hazen was CEO.

Sources: https://investor.hcahealthcare.com/

21. Welltok, 2023

What happened: Approximately 14.8 million people were affected by a ransomware incident involving a third-party file-transfer vulnerability.

How: The incident involved unauthorized access associated with a vulnerable file-transfer service.

Named suspects and countries: The sources summarized here do not establish a complete named perpetrator list.

Government connection: No government-directed operation has been established here.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: Executive and security leadership should be verified from the company's filings and notifications.

Sources: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

22. Change Healthcare, 2024

What happened: A ransomware attack disrupted healthcare claims and payment operations across the United States. The final reported notification total reached approximately 192.7 million people.

How: Attackers obtained unauthorized access and deployed ransomware, disrupting systems used by healthcare providers and pharmacies.

Named suspects and countries: The incident was attributed to the ALPHV/BlackCat ransomware operation. The identities, nationalities, and government affiliations of every participant in the operation are not established in this report.

Government connection: The incident is generally treated as criminal ransomware and extortion. No government-directed operation has been established here.

Arrests and wanted status: The report does not establish a specific arrest directly tied to the Change Healthcare attack. Any current arrest, indictment, or wanted status should be verified through official records.

Leadership: Andrew Witty was CEO of UnitedHealth Group.

Sources: https://www.unitedhealthgroup.com/ and https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Part V. Telecommunications and cloud services

23. T-Mobile, 2021 and 2023

What happened: The 2021 incident affected approximately 76.6 million U.S. consumers according to the FCC. A separate 2023 incident affected approximately 37 million accounts.

How: Attackers accessed customer information through separate incidents involving T-Mobile systems.

Named suspects and countries: The sources summarized here do not establish a complete verified list of individuals responsible for both incidents.

Government connection: No government-directed operation has been established in this report.

Arrests and wanted status: No specific arrest or current wanted status for both incidents is verified here.

Leadership: Mike Sievert was CEO.

Regulatory accountability: The FCC announced a $31.5 million settlement in 2024 covering investigations into multiple breaches.

Sources: https://www.fcc.gov/ and https://www.t-mobile.com/

24. AT&T, 2024

What happened: AT&T disclosed that call and text metadata from nearly all its customers over a six-month period in 2022 had been stolen from a third-party cloud platform. A separate disclosure involved customer information published on a criminal forum.

How: The incidents involved different access paths and data exposures. They must be recorded as separate cases.

Named suspects and countries: A complete, verified list of individuals responsible for each disclosure is not established here.

Government connection: No government-directed operation has been established in this report.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: John Stankey was CEO.

Sources: https://about.att.com/

25. Snowflake customer-account incidents, 2024

What happened: Attackers stole data from certain Snowflake customers, including AT&T, Ticketmaster/Live Nation, and Advance Auto Parts.

How: Investigations associated the incidents with compromised customer credentials and inadequate protections in some affected environments.

Named suspects and countries: A complete, verified list of named perpetrators responsible for the entire group of incidents is not established here.

Government connection: No single government-directed operation has been established for all the affected customer incidents. Each victim and intrusion must be assessed separately.

Arrests and wanted status: Current legal status must be checked separately for each incident.

Leadership: Michael Rapino was CEO of Live Nation.

Sources: https://www.snowflake.com/ and https://www.livenationentertainment.com/

Part VI. Other major corporate and technology incidents

26. Marriott and Starwood, 2014–2018

What happened: Attackers accessed Starwood's reservation database, exposing information from hundreds of millions of guest records.

How: Unauthorized access persisted in Starwood's environment before the breach was publicly disclosed after Marriott acquired Starwood.

Named suspects and countries: The sources summarized here do not establish a complete named perpetrator list for the incident.

Government connection: U.S. officials have attributed the Marriott incident to Chinese state-linked activity in broader public statements. The specific attribution should be tied to the relevant official assessment before assigning individual responsibility.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: Arne Sorenson was Marriott CEO when the breach was disclosed. Adam Aron led Starwood during part of the earlier period.

Sources: https://www.marriott.com/ and https://www.ftc.gov/

27. Sony Pictures Entertainment, 2014

What happened: Corporate files, employee personal information, unreleased films, and internal communications were stolen and leaked.

How: Attackers compromised corporate systems and released stolen data while disrupting operations.

Named suspects and countries: U.S. authorities attributed the operation to North Korea. This report does not establish a complete individually prosecuted perpetrator list for the incident.

Government connection: The U.S. government characterized the operation as associated with North Korea. The attribution should be distinguished from proof of the personal actions of any specific individual.

Arrests and wanted status: No specific arrest or current wanted status directly tied to the overall Sony Pictures incident is verified here.

Leadership: Michael Lynton was CEO of Sony Pictures Entertainment.

Sources: https://www.fbi.gov/ and https://www.sonypictures.com/

28. Home Depot, 2014

What happened: Approximately 56 million payment cards and 53 million email addresses were affected.

How: Attackers accessed payment systems and stole customer data.

Named suspects and countries: A complete, verified perpetrator list and country information are not established here.

Government connection: No government-directed operation has been established in this report.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: Frank Blake was CEO.

Sources: https://corporate.homedepot.com/

29. MOVEit Transfer, 2023

What happened: Attackers exploited a vulnerability in MOVEit Transfer, affecting thousands of organizations using the file-transfer software.

How: The campaign exploited a software vulnerability and was associated with the Clop extortion operation.

Named suspects and countries: The public attribution summarized here identifies the Clop operation, but does not establish a complete court-verified list of individual perpetrators and nationalities for every affected victim.

Government connection: No government-directed operation has been established in this report.

Arrests and wanted status: Legal status must be checked against current official notices and court records for each named suspect.

Sources: https://www.cisa.gov/ and https://www.progress.com/

30. National Public Data, 2024

What happened: Reports claimed that billions of records, including personal identifiers, were exposed. The claim of billions of records should not be treated as billions of unique individuals.

How: The exact origin, access method, and scope must be established through the relevant litigation, company records, and technical evidence.

Named suspects and countries: A complete verified list of named perpetrators and their government affiliations is not established here.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: The relevant executive and data-processing records should be verified for the incident period.

Sources: https://www.ftc.gov/ and https://pacer.uscourts.gov/

31. Microsoft corporate email, 2024

What happened: Microsoft reported unauthorized access to corporate email accounts.

How: Attackers accessed accounts and information in a separate incident from the 2021 Exchange Server vulnerability campaign.

Named group: Midnight Blizzard.

Country and government connection: Microsoft attributed the incident to a Russian state-sponsored group. That is a corporate attribution to a state-linked threat actor, not a finding that every participant has been individually identified or prosecuted.

Arrests and wanted status: A specific arrest or current wanted status directly tied to this incident is not established here.

Leadership: Satya Nadella was CEO.

Sources: https://www.microsoft.com/en-us/security

32. U.S. Department of the Treasury, 2024–2025

What happened: The Treasury Department disclosed unauthorized access involving a third-party remote-support service.

How: Attackers accessed systems through the third-party service.

Named suspects and countries: The department attributed the activity to a China state-sponsored actor. A complete individually prosecuted perpetrator list is not established here.

Government connection: The alleged perpetrators were associated with a foreign state-sponsored operation. The affected organization was a U.S. government department.

Arrests and wanted status: No specific arrest or current wanted status is verified here.

Leadership: The relevant Treasury Secretary, CIO, security leadership, and third-party provider leadership must be identified from the exact dates of the intrusion and disclosure.

Sources: https://home.treasury.gov/ and https://www.cisa.gov/

Part VII. Additional foreign state-linked cyber operations announced in 2025

33. Chinese contract hackers and alleged intelligence-linked operations

Public announcement: March 5, 2025.

What happened: The U.S. Department of Justice announced charges against 12 Chinese nationals in several investigations involving alleged global computer intrusion campaigns. The announcement covered different cases, including alleged activities involving i-Soon, Chinese law enforcement officers, and the APT27 group.

Named individuals and organizations: The announcement described eight employees of the Chinese company Anxun Information Technology, also known as i-Soon, and two alleged officers of China's Ministry of Public Security in one indictment. Separate indictments named Yin Kecheng and Zhou Shuai, also known as “Coldface,” in connection with alleged cyber intrusion campaigns.

Country and government connection: The defendants were identified as Chinese nationals. The U.S. government alleged that certain participants were Chinese government or law-enforcement officials and that private-sector contractors conducted operations at government direction.

Arrests and wanted status: The DOJ announcement stated that the defendants remained at large and wanted by the FBI at that time. The U.S. State Department also announced rewards for information leading to the identification or location of certain individuals involved in malicious cyber activity. These are historical statuses; a current wanted determination requires checking the live FBI notices.

Why: U.S. authorities alleged that the operations were used to gather sensitive information, target government agencies, journalists, religious organizations, and other entities, and suppress dissent.

How: The alleged operations involved hacking email accounts, phones, servers, and websites through a commercial hacker-for-hire ecosystem.

Sources:

- DOJ announcement: https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global
- FBI wanted notices: https://www.fbi.gov/wanted

34. Xu Zewei and the HAFNIUM-related investigation

Public announcement: July 8, 2025.

What happened: The U.S. Department of Justice announced that Xu Zewei had been arrested in Italy at the request of the United States. He and Zhang Yu were charged in connection with alleged intrusions between February 2020 and June 2021, including the HAFNIUM campaign.

Country and government connection: Both were identified as Chinese nationals. The indictment alleged that officers of China's Ministry of State Security directed the activity.

Arrest and legal status: Xu was arrested in Milan on July 3, 2025, and faced extradition proceedings at the time of the announcement. Zhang Yu was charged, but the cited announcement does not establish his arrest.

Important distinction: The Microsoft Exchange campaign affected thousands of computers worldwide. The case against Xu and Zhang is a particular criminal prosecution; it should not

be treated as proof that every HAFNIUM-associated intrusion was carried out by those two defendants.

Source: https://www.justice.gov/opa/pr/justice-department-announces-arrest-prolific-chinese-state-sponsored-contract-hacker

Part VIII. Perpetrator and legal-status summary

The following list consolidates the principal named suspects and legal developments documented above.

Incident	Named individual or group	Country or affiliation	Government connection	Documented status
Equifax	Wu Zhiyong, Wang Qian, Xu Ke, Liu Lei	China	Alleged People's Liberation Army members	Indicted in 2020; arrest not established in the cited announcement
Yahoo	Dmitry Dokuchaev, Igor Sushchin	Russia	Alleged FSB officers	Charged; described as fugitives in the 2017 announcement
Yahoo	Alexsey Belan	Russian national and resident; born in Latvia	Alleged criminal hacker working with FSB officers	Charged; described as fugitive and subject to an Interpol Red Notice at the time
Yahoo	Karim Baratov	Canadian and Kazakh national; resident of Canada	Criminal hacker alleged to have worked with FSB officers	Arrested in Canada; pleaded guilty and was sentenced
Twitter	Joseph O'Connor	British national; arrested in Spain	Criminal hacking case; no government direction established here	Arrested in Spain in 2021
Capital One	Paige Thompson	United States	Criminal intrusion case; no government direction established here	Arrested and prosecuted
Heartland and related payment card cases	Albert Gonzalez	United States	Criminal payment card hacking	Pleaded guilty in the broader cases
Microsoft Exchange/HAFNIUM-related case	Xu Zewei	China	Alleged Ministry of State Security-directed activity	Arrested in Italy in July 2025; extradition proceedings announced

Microsoft Exchange/HAFNIUM-related case	Zhang Yu	China	Alleged Ministry of State Security-directed activity	Charged; arrest not established in the cited announcement
2025 global cyber campaigns	Yin Kecheng, Zhou Shuai	China	Alleged APT27-linked activity	DOJ announced charges; defendants described as at large in the announcement
2025 global cyber campaigns	i-Soon employees and alleged officials	China	Alleged company and Ministry of Public Security connections	Charged; defendants described as at large in the announcement

The table does not constitute a complete global cybercrime wanted list. It includes only named individuals and legal developments specifically described in the report. A person may have a different current status following a later arrest, extradition, trial, conviction, or sentence.

Part IX. How to establish country and government involvement accurately

For each suspect, the final research file should record four separate facts:

Nationality: The country of citizenship when established by a reliable source.

Residence: The country where the person was reported to live at the time of the alleged offense.

Operational location: The physical location of the individual or the infrastructure used during the attack, when established. A server location or IP address does not by itself prove the attacker's physical location.

Government connection: Whether the individual was an employee, intelligence officer, military member, government contractor, alleged state-sponsored hacker, or apparently independent criminal.

These distinctions matter. A Russian national who operates a criminal hacking business is not automatically a Russian intelligence officer. A Chinese national accused of hacking is not automatically a member of China's government. Conversely, when an indictment specifically alleges that named defendants were intelligence or military officers acting under government direction, that allegation should be documented precisely and attributed to the prosecuting authority.

Part X. Primary-source research directory

U.S. Department of Justice: https://www.justice.gov/news
Criminal complaints, indictments, plea agreements, sentencing announcements, and extradition proceedings.

Federal Bureau of Investigation: https://www.fbi.gov/investigate/cyber
Cybercrime investigations, threat attribution, and wanted notices.

FBI cyber wanted list: https://www.fbi.gov/wanted/cyber
Official wanted-person notices and case-specific allegations.

INTERPOL: https://www.interpol.int/How-we-work/Notices
International notices. A Red Notice is a request for cooperation in locating and provisionally arresting a person pending extradition or similar legal action; it is not an international arrest warrant.

Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/
Technical advisories, vulnerability alerts, and incident guidance.

Government Accountability Office: https://www.gao.gov/
Audits and assessments of federal cybersecurity controls and oversight.

Federal Trade Commission: https://www.ftc.gov/news-events
Privacy enforcement, consumer protection proceedings, and corporate security findings.

HHS Office for Civil Rights: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
Healthcare breach notifications.

Privacy Rights Clearinghouse: https://privacyrights.org/data-breaches
Historical U.S. breach chronology.

Securities and Exchange Commission: https://www.sec.gov/edgar/search/
Corporate disclosures, executive statements, and risk filings.

Conclusion

A reliable national data breach report must document more than the name of a company or the number of affected records. It must identify the attack method, the alleged perpetrators, the countries and organizations associated with them, any documented government connections, and the legal outcome of the investigation. It must also identify the executives and security leaders responsible for the affected organization at the time, without confusing corporate accountability with proof of criminal conduct.

The cases in this report show several distinct patterns: criminal financial hacking, ransomware and extortion, credential theft, third-party data exposure, supply-chain compromise, and alleged state-sponsored intelligence operations. Each pattern requires its own evidence and legal analysis.

This report is an expanded starting register, not a fully verified, exhaustive database of every major U.S. breach. Entries marked as unverified require additional primary-source research before publication. In particular, current wanted status, country of residence, individual government affiliation, and the final outcome of criminal proceedings should be confirmed from official records and dated in the final version.

The objective is a documented, transparent record of who did what, when, where, why, and how, including what investigators established about government involvement and whether the people accused were arrested, convicted, or remained wanted.

Add a consistent incident templateSeparate verified facts from questions