CYBER THREAT SNAPSHOT

MALIGN NATION-STATES AND OPPORTUNISTIC CRIMINAL NETWORKS:
A PERSISTENT CYBER THREAT IN AMERICA

CHAIRMAN ANDREW R. GARBARINO

CYBERATTACKS ON STATE AND LOCAL GOVERNMENTS

SO FAR IN 2025, MAJOR CYBERATTACKS ON STATE AND LOCAL GOVERNMENTS HAVE BEEN OBSERVED IN AT LEAST 44 U.S. STATES.

STARTLING STATS

CHINESE MALICIOUS CYBER ACTIVITY SURGED BY 150% IN 2024 FROM THE PREVIOUS YEAR. Source: CrowdStrike

CHINESE ATTACKS TARGETED AGAINST FINANCIAL SERVICES, MEDIA, MANUFACTURING, AND THE INDUSTRIAL SECTORS INCREASED 300% FROM 2023 TO 2024. Source: CrowdStrike

THE AVERAGE COST OF A DATA BREACH IN THE U.S. REACHED $10 MILLION IN 2025, DOUBLE THE GLOBAL AVERAGE. Source: IBM

IRANIAN CYBERATTACKS SURGED 133% IN MAY AND JUNE 2025 COMPARED TO MARCH AND APRIL 2025.
Source: Nozomi Networks Labs

ONE IN SIX DATA BREACHES IN 2025 INVOLVED ATTACKS DRIVEN BY ARTIFICIAL INTELLIGENCE. Source: IBM

IN 2024, 70% OF CYBERATTACKS INVOLVED CRITICAL INFRASTRUCTURE. Source: IBM

SALT TYPHOON TARGETED 80 COUNTRIES AND POTENTIALLY GAINED ACCESS TO DATA FROM NEARLY EVERY AMERICAN.
Sources: Joint Cybersecurity Advisory; Federal Bureau of Investigation

NOTABLE RECENT THREAT ACTOR ACTIVITY

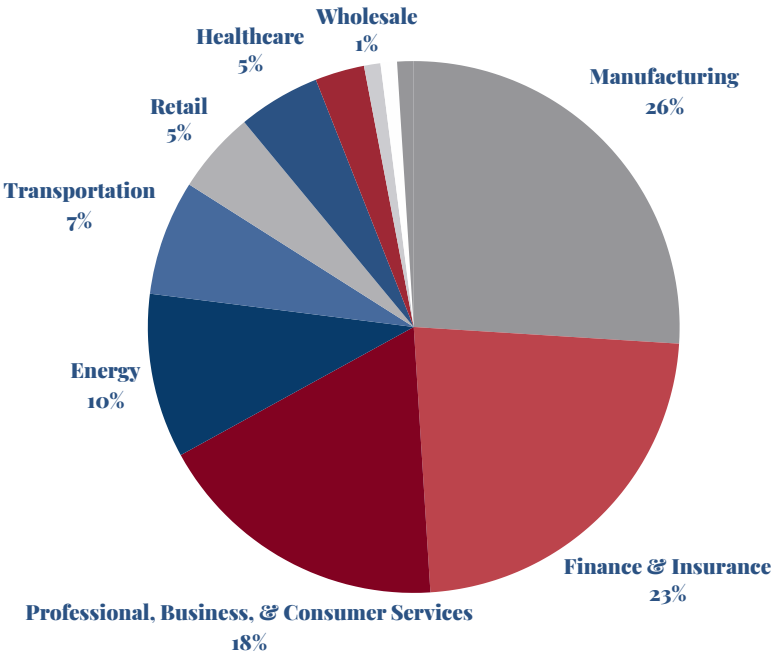
DPRK REMOTE IT WORKERS: DISCOVERED IN 2022, THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (DPRK) DEPLOYED UNDERCOVER INFORMATION TECHNOLOGY (IT) WORKERS TO INFILTRATE U.S. COMPANIES BY GAINING REMOTE IT JOBS.

SCATTERED SPIDER: DISCOVERED IN 2023, THIS DECENTRALIZED CYBERCRIMINAL ORGANIZATION USES RANSOMWARE AND DATA THEFT EXTORTION TO CONDUCT FINANCIALLY-MOTIVATED ATTACKS ON MAJOR GLOBAL COMPANIES.

INTERLOCK: DISCOVERED IN 2024, INTERLOCK, THE OPPORTUNISTIC, FINANCIALLY MOTIVATED THREAT ACTOR, CLAIMED RESPONSIBILITY FOR HIGH-PROFILE ATTACKS ON A LOCAL GOVERNMENT AND A LARGE MANUFACTURING COMPANY.

SALT TYPHOON: DISCOVERED IN 2024, THREAT ACTORS ASSOCIATED WITH THE PEOPLE'S REPUBLIC OF CHINA (PRC) INFILTRATED BACKDOORS IN MAJOR U.S. TELECOMMUNICATIONS COMPANIES, INCLUDING INTERNET SERVICE PROVIDERS.

GLOBAL CYBER INTRUSIONS BY SECTOR IN 2024



Source: IBM X-Force Threat Intelligence Index

2025

- **OCTOBER 2025: F5—**A U.S.-based enterprise technology vendor, F5, disclosed that a "highly sophisticated nation-state threat actor" breached the company's network, maintained long-term persistent access, and stole internal files that included source code and undisclosed vulnerabilities related to F5's BIG-IP product.[1] The Cybersecurity and Infrastructure Security Agency (CISA) issued a directive for all federal agencies to address the "unacceptable risk"[2] posed to federal systems and networks by this attack. As the investigation into the F5 breach is still ongoing, the attack is not yet officially attributed to a specific actor.
- **SEPTEMBER 2025: Cisco—**Cisco released an advisory to patch three critical zero-day vulnerabilities that were being actively exploited by a PRC-affiliated threat actor, Storm-1849/UAT4356.[3] This prompted CISA to issue a mandate to all federal agencies to patch their systems, given the "unacceptable risk to federal information systems."[4]
- **AUGUST 2025: State of Nevada—**A ransomware attack on the state government of Nevada caused significant disruptions in government services, including background checks, Department of Motor Vehicle services, the sex offender registry database, and access to most online services.[5] Due to the severity of the cyberattack, 10 percent of Nevada's public websites and services were still disrupted three weeks after the initial attack.[6]
- **JULY 2025: U.S. Department of Justice (DOJ)—**Russian-affiliated hackers reportedly breached the electronic case filing system used by the federal judiciary, which may have led the attackers to exfiltrate sealed case data from at least 12 district courts. According to media reports, the threat actors exploited vulnerabilities in the federal court filing system, CM/ECF, that were known and unpatched since at least 2020.[7]
- **JULY 2025: City of St. Paul, Minnesota—**The Interlock ransomware group attacked the local government of St. Paul, Minnesota, prompting the city to declare a state of emergency and completely shut down its networks for more than one month to prevent further damage. Numerous government services including online water bill payments, parks and recreation payment systems, and public internet terminals were affected by the cyberattack. After St. Paul officials refused to pay Interlock's ransom, the attackers publicly posted 43 gigabytes of data from the St. Paul Department of Parks and Recreation, a fraction of the 153 terabytes of data that hackers potentially accessed.[8]
- **JULY 2025: TransUnion—**The threat actor, ShinyHunters, exploited vulnerabilities in third-party Salesforce integrations to breach TransUnion, a credit reporting firm. According to TransUnion, this data breach impacted nearly 4.5 million U.S. individuals.[9]
- **JULY 2025: Microsoft SharePoint—**Three PRC-associated threat actors— Storm-2603, Linen Typhoon, and Violet Typhoon[10]—exploited vulnerabilities in Microsoft's on-premises SharePoint servers to compromise more than 400 organizations, including the Department of Energy (DOE), the Department of Homeland Security (DHS), and the Department of Health and Human Services (HHS).[11]
- **JUNE 2025: Scattered Spider Financial Attacks—**Scattered Spider, a decentralized cybercrime group comprised of young individuals from the United States and United Kingdom, launched cyberattacks against numerous U.S. companies, including Hawaiian Airlines,[12] Aflac,[13] and United Natural Foods.[14] The attack on United Natural Foods—Whole Foods Market's primary distributor—caused the company to completely shut down its networks for 10 days, resulting in financial losses up to $400 million.[15] Scattered Spider is a financially-motivated threat actor that uses ransomware and data theft extortion for monetary gain.[16]
- **APRIL 2025: Yale New Haven Health—**An unidentified actor breached the networks of Yale New Haven Health, Connecticut's largest healthcare provider, compromising the data of approximately 5.6 million individuals. The threat actor gained access to patient data, including but not limited to Social Security numbers, demographic information, and medical record numbers.[17]

- **APRIL 2025: Office of the Comptroller of the Currency—**Unidentified hackers gained unauthorized access to more than 103 email accounts for more than a year at the Department of the Treasury's Office of the Comptroller of the Currency (OCC), gaining visibility into approximately 150,000 emails from executives and employees.[18] According to the OCC, these emails contained "highly sensitive information relating to the financial condition of federally regulated financial institutions used in [the OCC's] examinations and supervisory oversight processes."[19]
- **MARCH 2025: National Presto Industries—**The Interlock ransomware group claimed responsibility for attacks on at least three subsidiaries of National Presto Industries, including the National Defense Corporation—a company that manufactures ammunition and explosives for the U.S. military and law enforcement. The ransomware group reportedly claimed responsibility for the theft of approximately 3 million files from the National Defense Corporation, although it is unclear whether the threat actor was able to successfully extort any money as a result of the attack.[20]
- **FEBRUARY 2025: City of Mission, Texas—**The city of Mission, Texas suffered a cyberattack that caused its main and backup servers to be encrypted by ransomware. The attack caused city officials to lose access to systems at every single city department, freezing critical records such as birth certificates, police reports, contracts, and personnel files. Mission officials declared a state of emergency in response to the ransomware attack.[21]
- **JANUARY 2025: Conduent—**A cyberattack targeting Conduent, a large government payments technology vendor for social services and transportation systems, caused significant disruptions in state government services and unauthorized access into client databases. Although it is unclear how many states were affected by this intrusion, Conduent is known to provide services to at least 37 state governments, so millions of individuals were potentially affected by the disruption and data breach. In Wisconsin, for example, the cyberattack impacted officials' ability to process child support payments through the Wisconsin Child Support Trust Fund.[22]

2024

- **DECEMBER 2024: RIBridges—**A threat actor by the name of Brian Cipher claimed responsibility for a ransomware attack against RIBridges, Rhode Island's social services platform, which exposed approximately 657,000 individuals' personal data. Affected data in the RIBridges database may include names, addresses, Social Security numbers, health information, dates of birth, phone numbers, and banking information.[23]
- **DECEMBER 2024: U.S. Treasury Department—**A PRC-associated threat actor gained unauthorized, remote access to U.S. Department of Treasury workstations and unclassified documents by stealing a third-party software provider's security key. This third-party provider, BeyondTrust, provided a cloud-based service to deliver remote technical support to the Treasury Department's staff offices. In the wake of the intrusion, the Treasury Department worked with CISA, the Federal Bureau of Investigation (FBI), the Intelligence Community, and third-party forensic investigators to determine the overall impact of the cyber incident.[24]
- **OCTOBER 2024: Salt Typhoon Infiltrations—**A threat actor associated with the PRC, Salt Typhoon, infiltrated backdoors in major internet service providers such as Verizon and AT&T to conduct espionage on law enforcement's wiretapping requests and potentially exfiltrate data.[25] This intrusion included accessing the phones of presidential candidates for surveillance purposes. The intrusion is still being investigated by authorities, but reports indicate phone call data and the locations of certain customers were potentially accessed, as well as call audio. There is no information available yet on how many calls were accessed, if so.[26]

- **OCTOBER 2024: American Water Works—**The networks of one of the country's major water utilities were breached by an unidentified cyber threat actor, forcing the company to shut down the online customer portal and billing services for days in an attempt to protect customer data.[27] The operational technology involved in water treatment operations was reportedly unaffected in the attack. The company provides services to more than 14 million Americans, including 18 military installations. The actor is unknown, although nation-state actors such as China, Iran, and Russia are known to target the sector.[28]
- **SEPTEMBER 2024: Flax Typhoon Intrusions—**PRC-affiliated actors Flax Typhoon burrowed into "Internet of Things" consumer products such as cameras and network-connected storage devices to conduct espionage on strategic organizations in Taiwan, as well as organizations on U.S. soil through the telecommunications sector, media companies, and higher education institutions.[29] The FBI successfully took down the botnet associated with Flax Typhoon in September 2024.[30]
- **SEPTEMBER 2024: Islamic Revolutionary Guard Corps Hacks—**Iran-backed hackers used spear-phishing to infiltrate the networks of the Trump campaign through a high-level staffer's email, and targeted government officials, lobbyists, think tanks, journalists, and Biden and Harris campaigns.[31] The DOJ indicted three Iranian nationals in the 'hack-and-leak' operation in September according to Microsoft.[32]
- **JUNE 2024: CDK Global—**A ransomware attack targeted a software firm serving 15,000 car dealerships in the United States.[35] This attack forced thousands of dealers across the country to conduct transactions and other crucial administrative tasks manually. The company reportedly paid a $25 million ransom to bring the systems back online, although that is not confirmed by CDK Global.[36]
- **MAY 2024: Ticketmaster—**The cybercriminal group ShinyHunters claimed responsibility for hacking Ticketmaster through its customer sales portal.[37] The website tried to shut down quickly, but more than 40 million accounts had data leaked onto a dark web forum used for further hacking attempts. Leaked data included contact information, biographical information, and payment data.[38]
- **MAY 2024: Ascension Hospitals—**A threat actor exploited known vulnerabilities after an employee downloaded malware from a phishing attempt,[39] impacting IT networks at all 142 Ascension hospitals in the United States and removing access to patient data in a ransomware attack.[40] The outages impacted patient care, led to rerouted ambulances, and delayed emergency services at numerous locations.[41]
- **APRIL 2024: AT&T—**AT&T notified the public that the private call and text data of millions of its cellular customers,[42] as well as some customers' locations at the time of use,[43] were breached and released on the dark web due to an intrusion into the third-party cloud storage provider, Snowflake.[44] Federal agencies were potentially among the customers at the time, including agencies within DHS.[45]
- **FEBRUARY 2024: UnitedHealth—**The UnitedHealth insurance company ransomware attack, allegedly by the threat actor BlackCat,[46] was the largest in the country and impacted 100 million people.[47] The intrusion was through a subsidiary payment processor, Change Healthcare. The company said the actor was potentially sponsored by a nation-state.[48] In Congressional testimony, United Health admitted they were not using multifactor authentication.[49] UnitedHealth paid $22 million in ransom to restore access to customer data, but the full impact cost the company upwards of $872 million.[50]
- **FEBRUARY 2024: LockBit Ransomware Disruption—**The DOJ and United Kingdom disrupted a variant of the LockBit ransomware group in 2024, which had targeted 2,000 victims and extorted $120 million in ransom payments across the globe since 2020.[51] Their targets included organizations and individuals working in the manufacturing and semiconductor industries. LockBit is a 'ransomware-as-a-service,' providing bad actors the ability to personalize the process and target through which they encrypt and steal data.[52]
- **JANUARY 2024: CISA—**A threat actor, presumed to be sophisticated, targeted CISA through zero-day vulnerabilities discovered in Ivanti Connect Secure virtual private network (VPN) for espionage.[53]

1. "K000154696: F5 Security Incident," MyF5, October 22, 2025, https://my.f5.com/manage/s/article/K000154696.

2. "ED 26-01: Mitigate Vulnerabilities in F5 Devices," U.S. Cybersecurity and Infrastructure Security Agency, October 15, 2025, https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices.

3. Atinderpal Singh et al., "Cisco Firewall and VPN Zero Day Attacks: CVE-2025-20333 and CVE-2025-20362," Zscaler Blog, September 26, 2025, https://www.zscaler.com/blogs/security-research/cisco-firewall-and-vpn-zero-day-attacks-cve-2025-20333-and-cve-2025-20362.

4. "ED 25-03: Identify and Mitigate Potential Compromise of Cisco Devices," U.S. Cybersecurity and Infrastructure Security Agency, September 25, 2025, https://www.cisa.gov/news-events/directives/ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices.

5. Oona Milliken and Eric Neugeboren, "A timeline of Nevada's cyberattack recovery," The Nevada Independent, September 12, 2025, https://thenevadaindependent.com/article/a-timeline-of-nevadas-cyberattack-recovery.

6. Keely Quinlan, "Cyberattack attempts on Nevada state websites increased 300% after August ransomware attack," StateScoop, September 12, 2025, https://statescoop.com/cyberattack-attempts-on-nevada-state-websites-increased-300-after-august-ransomware-attack/.

7. John Sakellariadis, "Hack of federal court filing system exploited security flaws known since 2020," August 12, 2025, https://www.politico.com/news/2025/08/12/federal-courts-hack-security-flaw-00506392.

8. Alex Derosier, "St. Paul, Minn., Systems Come Back Online After Cyber Attack," Government Technology, August 29, 2025, https://www.govtech.com/security/st-paul-minn-systems-come-back-online-after-cyber-attack.

9. Kurt Knutsson and CyberGuy Report, "TransUnion becomes latest victim in major wave of Salesforce-linked cyberattacks, 4.4M Americans affected," Fox News, August 31, 2025, https://www.foxnews.com/tech/transunion-becomes-latest-victim-major-wave-salesforce-linked-cyberattacks-4-4m-americans-affected.

10. Microsoft Threat Intelligence, "Disrupting active exploitation of on-premises SharePoint vulnerabilities," Microsoft, July 22, 2025, https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/.

11. Matt Kapko, "Microsoft SharePoint attacks ensnare 400 victims, including federal agencies," CyberScoop, July 24, 2025, https://cyberscoop.com/microsoft-sharepoint-attacks-400-victims-us-agencies/.

12. Anna Ribeiro, "FBI raises alarm over Scattered Spider targeting airline sector with social engineering schemes," Industrial Cyber, July 2, 2025, https://industrialcyber.co/transport/fbi-raises-alarm-over-scattered-spider-targeting-airline-sector-with-social-engineering-schemes/.

13. Steve Weisman, "Aflac Data Breach By Scattered Spider Hackers Is No Quacking Matter," Forbes, June 21, 2025, https://www.forbes.com/sites/steveweisman/2025/06/21/aflac-data-breach-by-scattered-spider-hackers-is-no-quacking-matter/.

14. Matt Kapko, "United Natural Foods loses up to $400M in sales after cyberattack," CyberScoop, July 17, 2025, https://cyberscoop.com/united-natural-foods-cyberattack-400-million/.

15. Ibid.

16. Flashpoint Intel Team, "Scattered Spider: A Threat Profile," Flashpoint, August 15, 2025, https://flashpoint.io/blog/scattered-spider-threat-profile/?CRO3=%233007_control.

17. Emily Olsen, "Data breach at Yale New Haven Health impacts 5.6M people," Healthcare Dive, April 24, 2025, https://www.healthcaredive.com/news/yale-new-haven-health-data-breach-5-6-million/746236/.

18. Elizabeth Montalbano, "Treasury Department bank regulator discloses major hack," Cybersecurity Dive, April 9, 2025, https://www.cybersecuritydive.com/news/treasury-department-office-overseeing-bank-regulations-hacked/744871/.

19. "OCC Notifies Congress of Incident Involving Email System," U.S. Department of the Treasury, Office of the Comptroller of the Currency, April 8, 2025, https://occ.gov/news-issuances/news-releases/2025/nr-occ-2025-30.html.

20. Ionut Arghire, "Ransomware Group Takes Credit for National Presto Industries Attack," SecurityWeek, April 1, 2025, https://www.securityweek.com/ransomware-group-takes-credit-for-national-presto-industries-attack/.

21. "City of Mission Catastrophe Notice," Ken Paxton, Attorney General of Texas, March 1, 2025, https://statescoop.com/mission-texas-state-emergency-cyberattack-2025/.

22. David Jones, "Conduent warns January breach impacted a 'significant' number of people," Cybersecurity Dive, April 22, 2025, https://www.cybersecuritydive.com/news/conduent-breach-significant-number/745963/.

23. David Jones, "Hack of Rhode Island social services platform impacted at least 709K, officials say," Cybersecurity Dive, January 10, 2025, https://www.cybersecuritydive.com/news/rhode-island-social-services-breach-709k/737111/.

24. Aditi Hardikar, "Letter to Chairman Brown and Ranking Member Scott," U.S. Department of the Treasury, December 30, 2024, https://legacy.www.documentcloud.org/documents/25472740-letter-to-chairman-brown-and-ranking-member-scott/.

25. Ellen Nakashima and Josh Dawsey, "Chinese hackers said to have collected audio of American calls," The Washington Post, updated October 27, 2024, https://www.washingtonpost.com/national-security/2024/10/27/chinese-hackers-cellphones-trump/.

26. Jessica Lyons, "Feds investigate China's Salt Typhoon amid campaign phone hacks," The Register, October 28, 2024, https://www.theregister.com/2024/10/28/feds_investigate_chinas_salt_typhoon/.

27. Kate Gibson, "Water supplier American Water Works says systems hacked," CBS News, October 8, 2024, https://www.cbsnews.com/news/security-hack-breach-american-water-works/.

28. Sean Michael Kerner, "The American Water cyberattack: Explaining how it happened," TechTarget, October 18, 2024, www.techtarget.com/whatis/feature/The-American-Water-cyberattack-Explaining-how-it-happend.

29. Sam Sabin, "Chinese hacking 'typhoons' threaten U.S. infrastructure," Axios, September 20, 2024, https://www.axios.com/2024/09/20/china-critical-infrastructure-cyberattacks.

30. Cate Burgan, "Wray: FBI Takes Down Chinese 'Flax Typhoon' Hacker Botnet," MeriTalk, September 18, 2024, https://www.meritalk.com/articles/wray-fbi-takes-down-chinese-flax-typhoon-hacker-botnet/.

31. Federal Bureau of Investigation, U.S. Cyber Command, Cyber National Mission Force, the Department of the Treasury, and National Cyber Security Centre, government advisory, September 2024, https://www.ic3.gov/CSA/2024/240927.pdf.

32. U.S. Department of Justice, "Three IRGC Cyber Actors Indicted for 'Hack-and-Leak' Operation Designed to Influence the 2024 U.S. Presidential Election," press release, September 27, 2024, https://www.justice.gov/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us.

33. Tim Starks, "Iranian hackers 'tickle' targets in US, UAE with custom tool, Microsoft says," CyberScoop, August 28, 2024, https://cyberscoop.com/iranian-hackers-tickle-targets-in-us-uae-with-custom-tool-microsoft-says/.

34. Ibid.

35. Ananta Agarwal, "Why a hack at CDK Global is casting a shadow on US auto sales," Reuters, July 1, 2024, https://www.reuters.com/technology/cybersecurity/why-hack-cdk-global-is-casting-shadow-us-auto-sales-2024-07-01.

36. Sean Lyngaas, "How did the auto dealer outage end? CDK almost certainly paid a $25 million ransom," CNN Business, July 11, 2024, https://www.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html.

37. "Hacking group claims it breached Ticketmaster and stole data for 560 million customers," CBS News, May 30, 2024, https://www.cbsnews.com/news/ticketmaster-breach-shinyhunters-560-million-customers/.

38. Framework Security, "Ticketmaster Breach: A Deep Dive into the May 2024 Cyberattack and the History of the Alleged Hackers," June 28, 2024, https://www.frameworksec.com/post/ticketmaster-breach-a-deep-dive-into-the-may-2024-cyberattack-and-the-history-of-the-alleged-hackers.

39. Emily Olsen, "Ascension says cyberattack may have compromised protected health data," Cybersecurity Dive, June 14, 2024, https://www.cybersecuritydive.com/news/ascension-cyberattack-health-data-exposed/718978/.

40. Steve Alder, "Ascension Ransomware Attack Hurts Financial Recovery," The HIPAA Journal, September 20, 2024, https://www.hipaajournal.com/ascension-cyberattack-024.

41. Olivia Aldridge, "How the Ascension cyberattack is disrupting care at hospitals," NPR, May 23, 2024, https://www.npr.org/sections/shots-health-news/2024/05/23/1253011397/how-the-ascension-cyberattack-is-disrupting-care-at-hospitals.

42. AT&T, "AT&T Addresses Illegal Download of Customer Data," press release, July 12, 2024, https://about.att.com/story/2024/addressing-illegal-download.html.

43. Ryan Gallagher, "AT&T Hack Undermines US National Security, Experts Say," Bloomberg News, July 12, 2024, https://www.bloomberg.com/news/articles/2024-07-12/at-t-hack-undermines-us-national-security-experts-say.

44. David DiMolfetta, "Dozens of federal agencies' call data potentially exposed in AT&T breach," NextGov/FCW, July 12, 2024, https://www.nextgov.com/cybersecurity/2024/07/dozens-federal-agencies-call-data-potentially-exposed-t-breach/398005/.

45. Ibid.

46. Ashley Capoot, "Ransomware group Blackcat is behind cyberattack on UnitedHealth division, company says," CNBC, updated February 29, 2024, https://www.cnbc.com/2024/02/29/blackcat-claims-responsibility-for-cyberattack-at-unitedhealth.html.

47. Noah Barsky, "UnitedHealth Paid Hackers $22 Million, Fixes Will Soon Cost Billions," Forbes, updated June 7, 2024, https://www.forbes.com/sites/noahbarsky/2024/04/30/unitedhealths-16-billion-tally-grossly-understates-cyberattackcost/.

48. Darius Tahir, "Hacking at UnitedHealth unit cripples a swath of the U.S. health system: What to know," CBS News, February 29, 2024, https://www.cbsnews.com/news/unitedhealth-cyberattack-cloud-based-network-cybersecurity/.

49. House Energy and Commerce Committee, "What We Learned: Change Healthcare Cyber Attack," press release, May 3, 2024, https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack.

50. Khristopher J. Brooks, "UnitedHealth says Change Healthcare cyberattack cost it $872 million," CBS News, updated April 18, 2024, https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-hack-ransomware/.

51. U.S. Department of Justice, "U.S. and U.K. Disrupt LockBit Ransomware Variant," press release, February 20, 2024, https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant.

52. Ibid.

53. U.S. Cybersecurity and Infrastructure Agency (CISA), Cybersecurity Advisory: Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways, government advisory, February 29, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b.