REPORT

Defending the Federal Supply Chain:

A Cyber Security Assessment of the Top 100 U.S. Government Contractors

SecurityScorecard

Introduction

Federal contractors are critical to the U.S. Government's (USG) supply chain, yet their cybersecurity postures reveal significant weaknesses. This report evaluates the **SecurityScorecard ratings** and publicly available breach histories of the top 100 federal contractors for FY2023, highlighting problems and patterns that pose substantial third-party cyber risks to the USG. A breach at one of these contractors could expose USG data, compromise infrastructure, or disrupt essential products and services.

Despite the high stakes, the measurable security posture of these contractors is no better than that of the U.S. private sector on average. In fact, two recent private-sector samples outperformed these contractors. Given their roles and the sensitivity of their work, federal contractors should meet higher standards, yet this does not appear to be the case.

This insufficiently robust security posture may explain why:

Cybersecurity Assessment of the Top 100 U.S. Government Contractors

35%

of contractors reported publicly known breaches

14%

experienced multiple breaches

28%

showed signs of recent infections or compromises

Third-party breaches play an outsized role, accounting for **58% of incidents**—double the global average of **29%.** While **state-sponsored groups** are often assumed to be the most significant threat, they accounted for only **35%** of attributable breaches. However, for third-party breaches specifically, that figure rose to **39.5%,** making third-party breaches a particular area of concern. Third-party breaches at these contractors are also more likely to affect USG equities: only **15%** of all breaches in our sample affected USG equities, but that figure rose to **26%** in third-party breaches. Ransomware operators also represent a serious threat, responsible for **41.25%** of all attributable breaches in this sample and **46.5%** of attributable third-party breaches. Their ability to exploit third-party vulnerabilities underscores the urgent need to address risks within the federal supply chain.

Concepts and Methodology

The distribution of federal contract spending among a relatively small number of organizations introduces a significant layer of **concentration risk.** This phenomenon mirrors findings from our analysis of the top 150 technology vendors, where a small group of companies controls a large share of the market for technology products and services. In those cases, a compromise or disruption of just one top vendor could have widespread supply chain impacts. Similarly, within the federal contractor ecosystem, the compromise of a contractor with a substantial market share could have far-reaching consequences for the U.S. Government (USG), disrupting critical operations and services.

Analysis of USG statistics illustrates the extent of this concentration:

- The **top 100 federal contractors** account for **65% of all contract actions and 56% of total contract spending.**
- A single top contractor represents more than **9% of all spending.**
- The **top 10 contractors** collectively account for **29% of spending** and **34% of contract actions.**

These statistics highlight the systemic risks posed by this reliance, where vulnerabilities in a single organization could ripple across the broader USG supply chain.

To provide a comprehensive assessment of these contractors, we analyzed the following data points for each of the top 100 organizations:

1. **Overall security scores,** derived from SecurityScorecard's non-intrusive scanning and evaluation of their publicly accessible attack surfaces and breach histories.
2. The **lowest sub-scores** in key security risk factors, highlighting their most critical vulnerabilities.
3. The **specific issue** that had the greatest negative impact on their overall scores.
4. **Evidence of compromised devices** or malware infections detected within the past year.
5. **Publicly reported breaches**, including whether these breaches involved third-party attack vectors and their potential effects on the USG or other impacted entities.

This structured methodology not only identifies the systemic challenges of concentration risk but also pinpoints the individual weaknesses within contractors' security postures. Such insights are vital for mitigating cascading risks and ensuring the security of the federalsupply chain.

Key Findings

The top 100 federal contractors' security ratings are similar to much of the U.S. private sector.

However, the S&P 500 and the U.S. healthcare & pharmaceutical industry performed better. Both had higher average scores and more organizations with strong letter grades.

Security Ratings by Industry

Security scores vary widely by industry. Contractors working in **defense, intelligence, and national security** had the highest average scores. These sectors manage the most sensitive USG contracts. The lowest scores came from **technology and telecommunications companies, universities, and state or foreign governments.**

Primary Risk Factors

Application Security:

The most common area of risk, with **41%** of contractors scoring lowest here.

46% of the most negative issues affecting scores came from Application Security problems. This trend is consistent with other private sector samples.

DNS Health and Patching Cadence

DNS Health ranked higher than usual as a risk factor compared to other industries.

Patching Cadence, rarely a top issue in other sectors, ranked third for this group. Delays in addressing known vulnerabilities contribute to this risk.

Compromises and Breaches

- **28%** of contractors had at least one malware infection or compromised device on their networks in the past year. This is higher than in most private sector samples.
- **35%** of contractors experienced publicly reported breaches:
  - 14% had multiple breaches (2–5 incidents each).
  - One contractor experienced five breaches, and another experienced four.

Products and Services Enabling Breaches

The top three categories contributing to third-party breaches were:

1. Technology and telecommunications.
2. Healthcare.
3. HR, recruiting, and benefits.

Third-Party Breaches

- 58% of breaches involved third-party attack vectors. This is double the global average of 29%.
- Only 26% of third-party breaches affected USG operations, but these incidents still pose a serious risk.

Threat Actor Attribution

- **State-sponsored groups** were responsible for 35% of breaches attributed to specific actors.
- **Ransomware operators** accounted for a larger share of breaches (41.25%) and an even larger share of third-party breaches (46.5%). Less sophisticated attackers, such as hacktivists, are less likely to use third-party attack vectors.

These findings highlight significant risks for contractors, particularly in Application Security, DNS Health, and Patching Cadence. Addressing these vulnerabilities is critical to reducing the threat of malware, breaches, and third-party attacks.

Security Ratings of the Top 100 Federal Contractors

The average (mean) security score for the top **100** federal contractors is **86 out of 100**, while the median score is **88**. The lower mean score reflects the impact of a few contractors with significantly lower scores pulling the average down.

These scores are better than the global average of **82** across **12 million** organizations worldwide. They are comparable to other industries analyzed by SecurityScorecard:

U.S. energy industry: **86** (mean)/**88** (median).

Global aviation industry: **85/88**.

Top 150 technology vendors: **84/87**.

However, these scores fall below the U.S. healthcare & pharmaceuticals industry and the S&P 500, both of which scored **88/89**.

Given the sensitive work many federal contractors perform for the U.S. Government (USG), one might expect them to have higher security scores than other private-sector organizations. Instead, their scores are similar to, or lower than, many private sector benchmarks.

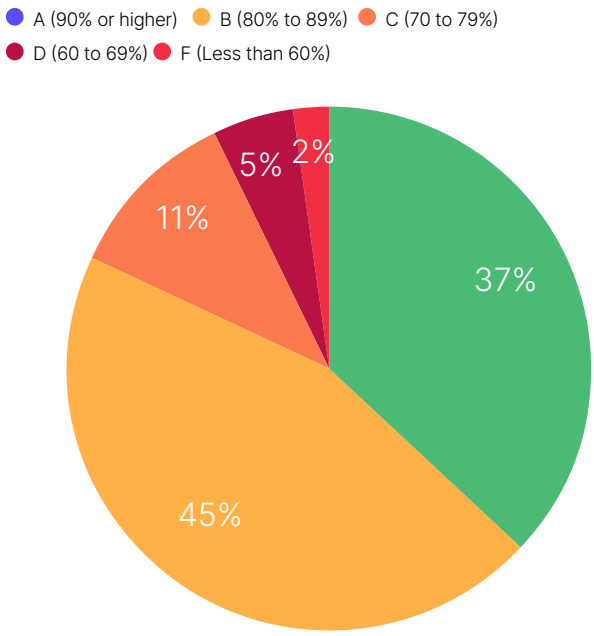
According to the SecurityScorecard rating system:

A "B" rating increases the likelihood of a breach by **2.9** times compared to an "A."

A "C" rating increases breach likelihood by **5.4** times.

A "D" rating increases it by **9.2** times, and an "F" rating by **13.8** times.

LETTER GRADE DISTRIBUTION FOR TOP 100 CYBER SECURE FEDERAL CONTRACTORS



In this sample, **82% of contractors received A or B ratings**, indicating strong or respectable security postures. Only **18%** scored C, D, or F, reflecting weaker security. This aligns closely with the U.S. energy industry, where **81%** of organizations achieved A or B ratings. It also outperforms global aviation (77%) and top technology vendors (77%). However, it still lags behind the S&P 500 (88%) and U.S. healthcare and pharmaceuticals (90%).

This data reveals a mixed picture: while most contractors show strong or adequate security, their overall performance does not reflect the elevated standards expected for organizations handling sensitive USG work. The few contractors with low ratings represent a disproportionate risk, emphasizing the need for targeted improvements.

Variations by Industry

We divided the top 100 federal contractors into six categories in order to determine how their security ratings vary. These categories reflect differences in their reliance on federal contracts. Some, especially in the first group, focus almost entirely on federal work. Others are more commercially oriented, with federal contracts as just one part of their broader business.

DEFENSE, INTELLIGENCE, AND MILITARY AEROSPACE

These companies serve the national security needs of the Department of Defense (DoD) and the Intelligence Community (IC). Their work includes military hardware, specialized software, IT services, and civilian staff support. Examples include **Lockheed Martin, Northrup Grumman, and RTX.**

TECHNOLOGY & TELECOMMUNICATIONS

Primarily commercial companies, these contractors also serve the USG with IT and telecom services. Examples include **Microsoft, Dell, IBM, and AT&T.**

ENGINEERING, ENERGY, AND CIVILIAN AEROSPACE

This group supports civilian-focused agencies like the Department of Energy (DoE) and NASA. Their contracts cover nuclear technology, space exploration, and public engineering projects. Some also support DoD research and development (R&D). Examples include **General Electric, Honeywell, and SpaceX.**

PROFESSIONAL, FINANCIAL, AND LOGISTICAL SERVICES

This category includes professional services firms and logistics providers. Examples include **Booz Allen Hamilton,** the "Big 4" accounting firms, and **Federal Express.** Financial services providers, such as **StoneX,** also fall into this category.

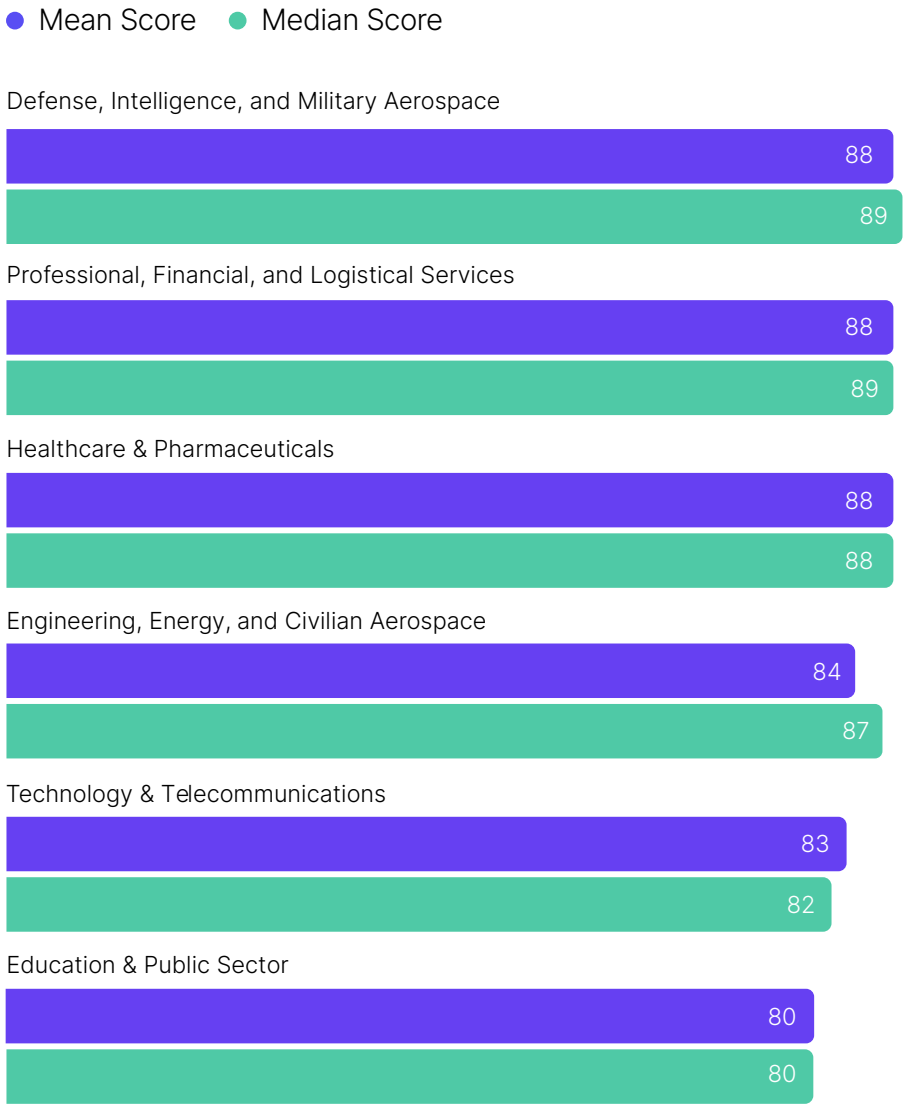
HEALTHCARE & PHARMACEUTICALS

These contractors work with agencies like the Department of Health and Human Services (HHS) and the Department of Veterans Affairs (VA). Their work includes healthcare delivery, pharmaceuticals, and public health initiatives like COVID-19 prevention. Examples include **Pfizer, Humana, and TriWest Healthcare Alliance.**

EDUCATION & PUBLIC SECTOR

This group includes universities and state or foreign governments. Examples are the **Massachusetts Institute of Technology,** the California Institute of Technology, and the governments of **California** and **Canada.**

Mean and Median Scores by Industry



Key Observations

High-Scoring Categories:

Contractors handling the most sensitive national security work, such as those in **Defense, Intelligence, and Military Aerospace,** achieved the highest scores. Their strong ratings align with their critical roles.

Professional, Financial, and Logistical Services also scored high, reflecting their strong compliance cultures and regulatory oversight.

Mid-Level Performance:

Healthcare & Pharmaceuticals reported solid scores, despite frequent ransomware attacks and breaches in the healthcare sector. This perfomance is likely due to the robust security measures of pharmaceutical companies protecting valuable intellectual property.

Low-Scoring Categories:

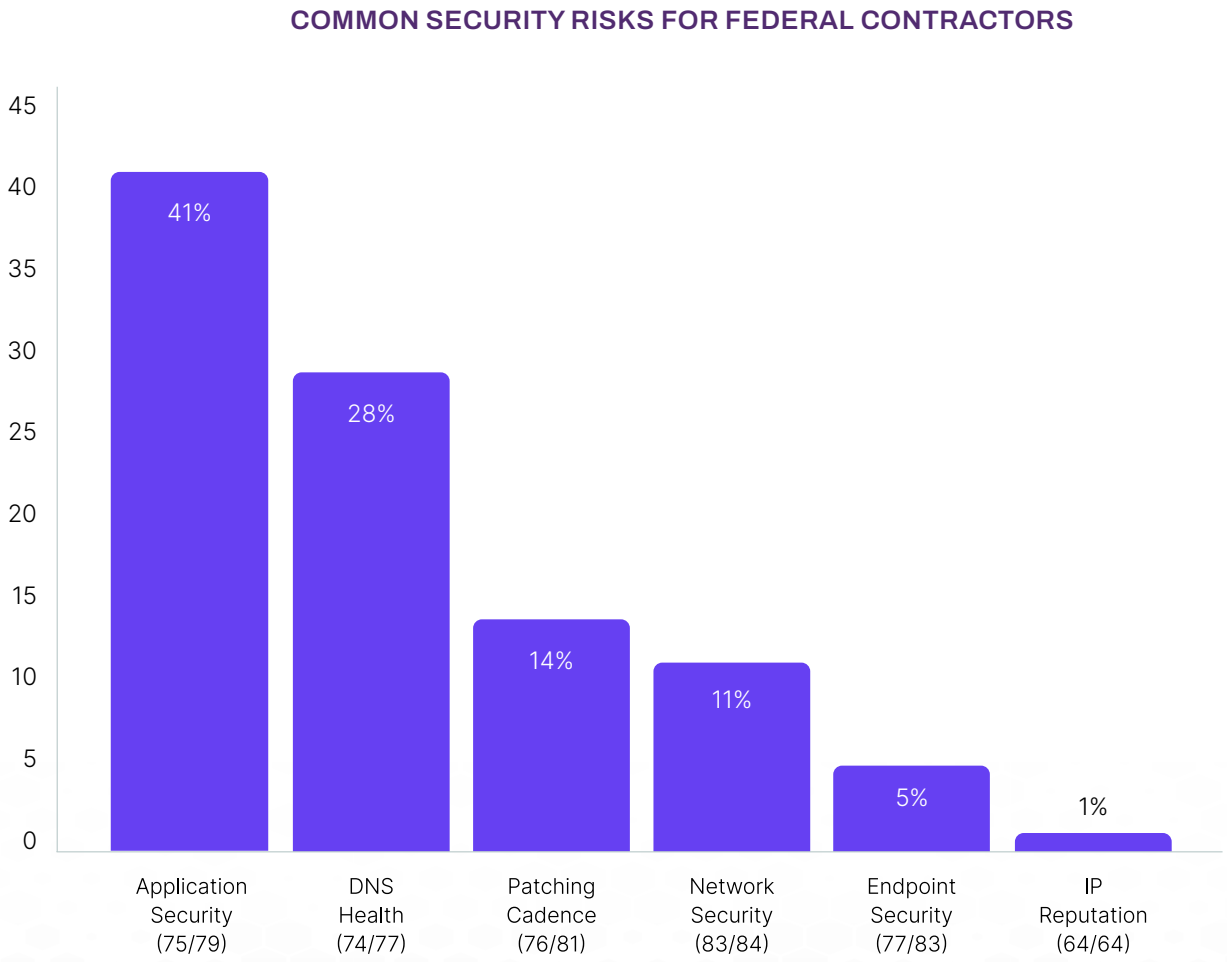
Technology & Telecommunications scored lower due to their large, complex, and exposed attack surfaces. Retail customers controlling devices, such as routers, add to the risks for telecom providers.

Education & Public Sector scored the lowest. Challenges for universities include limited funding, low security awareness, and open-access environments like computer labs. State and local governments face similar issues with restricted budgets for cybersecurity.

These variations underscore how the nature of an industry influences its security posture. Contractors in critical national security roles tend to score higher, while those with broader commercial operations or limited resources often face greater risks.

Common Security Risks

For each of the top 100 contractors, we identified the security factor where they received their lowest sub-score. Below are the percentages of contractors scoring lowest in each category, along with their mean and median scores:



Key Observations

Application Security was the weakest area for 41% of contractors, far outpacing other categories. Nearly half (46%) of the most impactful security issues also stemmed from Application Security. This trend is consistent across many industry samples.

DNS Health, while often a common weakness, ranked second with an unusually high percentage. Contractors with low scores in this category had some of the lowest averages, second only to IP Reputation.

Patching Cadence, which rarely ranks prominently in private sector samples, was the third most common source of risk. This highlights delays in applying critical updates.

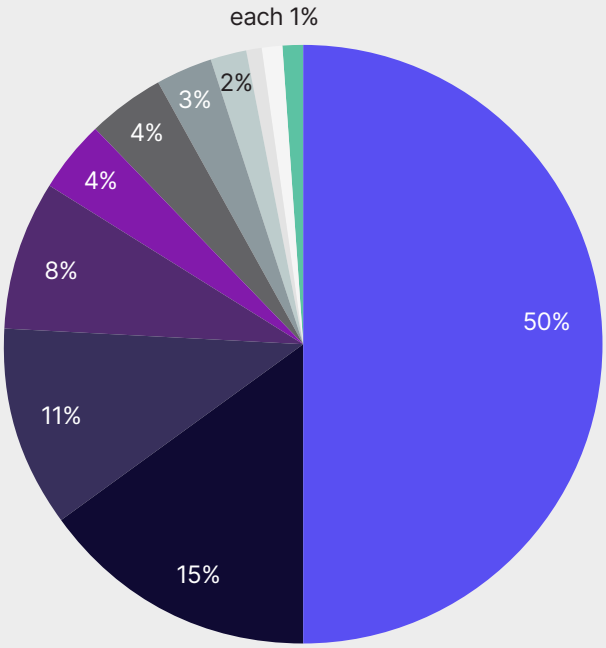
Network Security and **Endpoint Security** appeared less frequently as problem areas but had the highest mean and median scores among the lowest sub-scores.

Detailed Security Issues

We also examined the specific issues that had the greatest negative impact on scores. Below are the percentages of each issue and their associated category:

SECURITY ISSUES WITH MOST NEGATIVE SCORE IMPACT FOR EACH CONTRACTOR

- Weak SSL/TLS Protocols (Network Security): 50%
- HTTP in Redirect Chains (Application Security): 15%
- Session Cookies Missing 'Secure' Attribute (Application Security): 11%
- Website References Object Storage (Application Security): 8%
- Session Cookies Missing 'HTTPOnly' Attribute (Application Security): 4%
- Outdated Web Browsers (Endpoint Security): 4%
- Unsafe Subresource Integrity (Application Security): 3%
- Missing SPF Record (DNS Health): 2%
- Website Communicating with Payment Provider (Application Security): 1%
- Revoked Certificates (Network Security): 1%
- Detected HTTP Proxy Service (Network Security): 1%



Insights by Issue

- **Weak SSL/TLS Protocols** were the most common issue, appearing in 50% of cases. These involve outdated libraries, weak cryptographic algorithms, or misconfigurations, which leave systems vulnerable to attacks. This problem frequently appears across various industry analyses.
- **HTTP in Redirect Chains** was the leading Application Security issue, affecting 15% of contractors. Using HTTP instead of HTTPS in redirects exposes data to interception and increases the risk of phishing or other malicious attacks.
- **Session Cookies Without 'Secure' or 'HTTPOnly' Attributes** weaken protection against attacks like interception and cross-site scripting (XSS). This lack of controls makes session hijacking easier for attackers.
- **Object Storage Misconfigurations** allow unauthorized access to cloud-stored data. Poorly configured access control lists (ACLs) are a common source of this issue.
- **Missing SPF Records** were the only DNS Health issue on the list. SPF records help prevent email spoofing by defining the servers authorized to send messages for a domain. Their absence increases the risk of email spoofing.

The prevalence of Application Security as the weakest factor highlights a critical area for improvement. DNS Health and Patching Cadence also emerged as prominent vulnerabilities, with contractors scoring poorly in these areas compared to other industry samples. Addressing these specific issues, particularly weak SSL/TLS protocols and HTTP usage in redirects, can significantly strengthen overall security and reduce risk.

Malware Infections and Compromised Devices

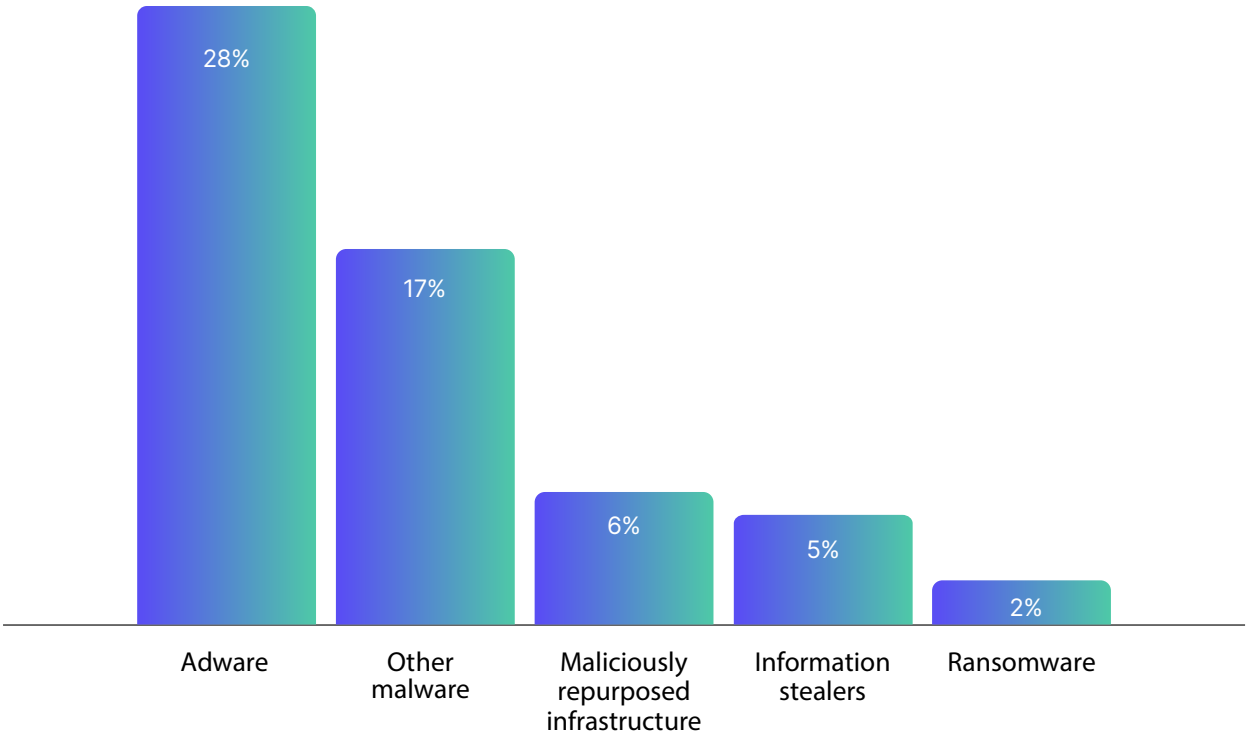
The **IP Reputation** security factor identifies signs of potential malware infections or device compromises over the past year. This data is gathered from sources like sinkholes and honeypots, revealing infections with ransomware, adware, information stealers, and other malware. It also includes cases where compromised devices were repurposed for malicious purposes, such as launching attacks, running scans, or supporting the TOR anonymity network.

These findings do not always indicate a large-scale breach. Often, they simply reflect a single compromised device. However, such signals can reveal undetected breaches or provide early warnings of weaknesses that could be exploited further. A single compromised device might serve as an entry point for attackers to expand access within the network.

Our analysis found that **28 out of the top 100 contractors** showed evidence of at least one malware infection or compromised device in the past year. This **28% compromise rate** is significantly higher than in other industries:

- **Global aviation industry: 17%**.
- **U.S. energy sector: 8%.**
- Only the **top 150 technology vendors** had a higher infection rate at **41%**.

Specific types of infections or compromises were distributed as follows:



Publicly Reported Breaches

Reports from sources like media outlets, lawsuits, corporate filings, government disclosures, and criminal forums provided further insights into breaches. These breaches are critical for evaluating correlations between compromised signals and actual incidents. Additionally, breaches impact security scores, as organizations with a history of incidents pose higher risks. Publicly disclosed breaches often include sensitive technical details, such as credentials or reconnaissance data, that other attackers can exploit.

The two contractors with four and five breaches accounted for 15% of all breaches in this sample. The overall breach rate of 35% is high, particularly for organizations handling sensitive national security data. By comparison, the U.S. energy industry showed a breach rate of only 14% among its top 250 organizations.

Our findings revealed:

60 publicly reported breaches affecting **35 of the 100 Contractors**

21 experienced one breach

12 Contractors experienced Multiple Breaches

- **6** Had **two** breaches
- **6** Had **three** breaches
- **1** Had **four** breaches
- **1** Had **five** breaches

Third-Party Breaches

Of the **60 publicly reported breaches, 35 (58%)** involved third-party vectors. This rate is **double the global average of 29%** and higher than the **45% third-party breach rate** observed in the U.S. energy sector.

Third-party breaches occur when:

1. Infrastructure or data belonging to another organization is compromised.
2. An attack vector from a vendor, partner or other third party enables a breach.

While concerning, only **9 of the 60 breaches** directly impacted the USG. These **9 breaches** accounted for **15% of the total breaches and 26% of the third-party subset**. Other third-party breaches affected contractors' commercial customers, internal systems, or other parties without direct USG connections.

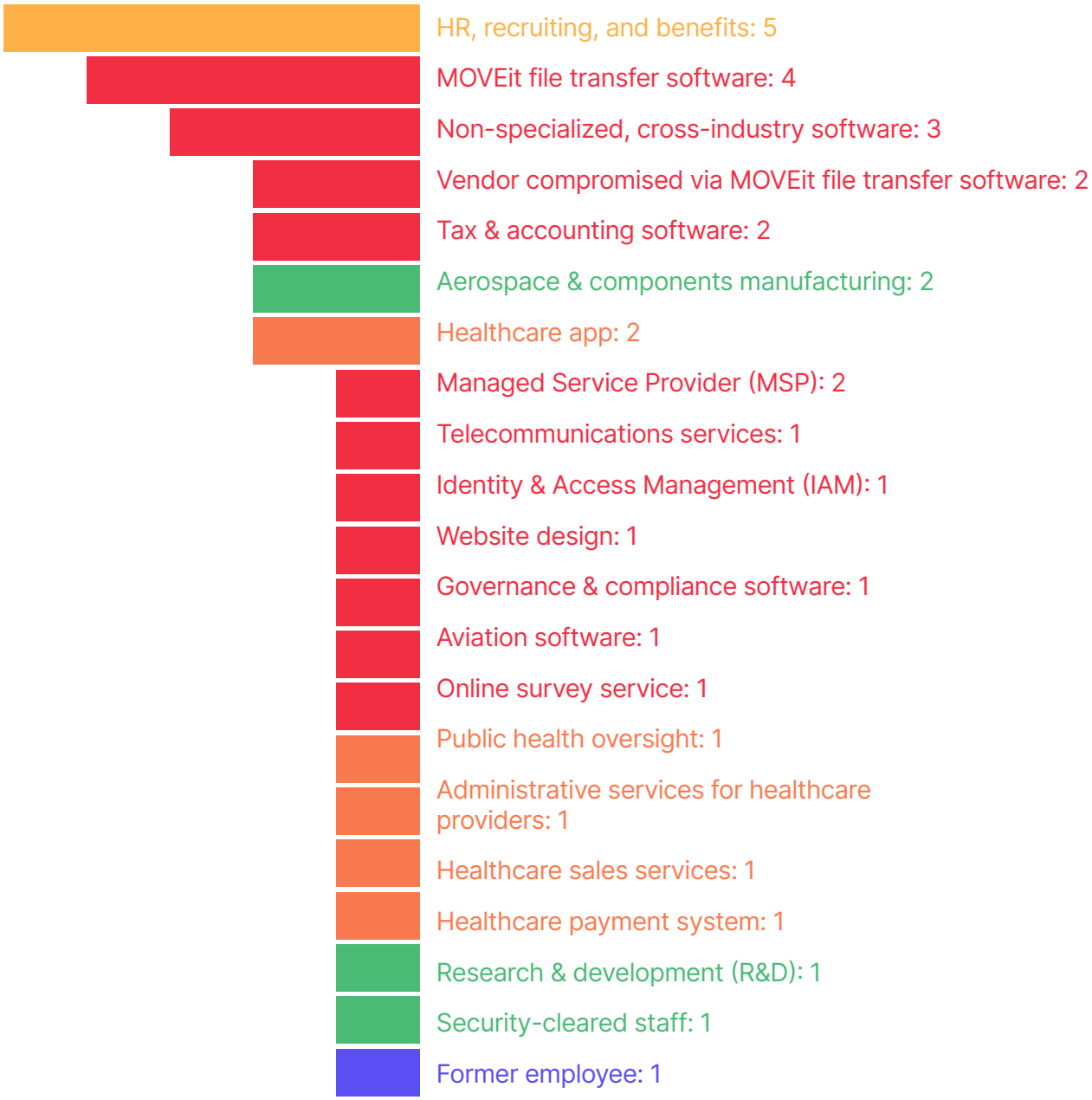
Several factors reduce the impact of third-party breaches on the USG:

- Contractors with critical national security work often use network air gaps and segmentation to protect sensitive systems.
- Many breaches targeted commercial segments of contractors, which are unrelated to their federal contracts.

Types of Relationships That Enable Third-Party Breaches

Analysis of the **35 third-party breaches** revealed the following types of vendor relationships that contributed to the incidents:

PRODUCTS AND SERVICES ENABLING THIRD-PARTY BREACHES



Categories of Vendor Relationships by Breach Proportion:

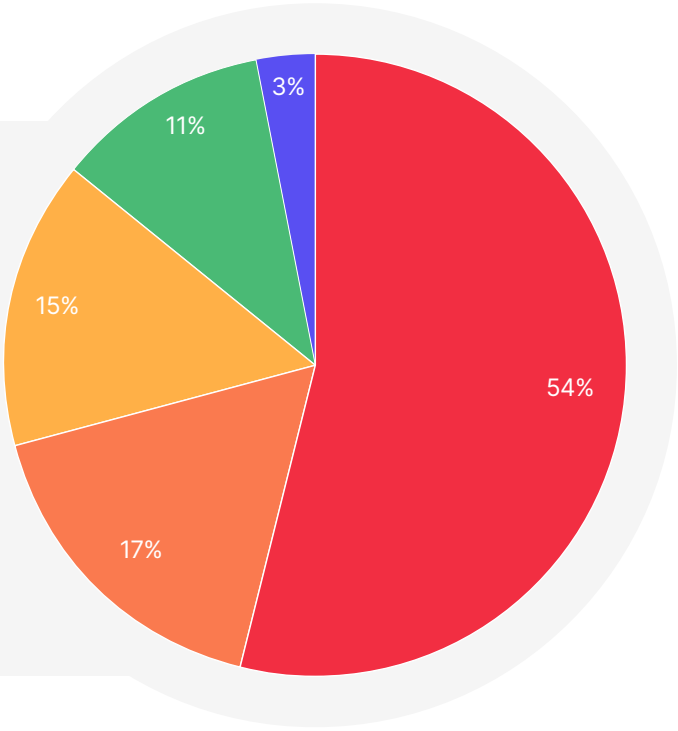
Technology & Telecommunications: 54%. Includes services like managed service providers (MSPs), IAM solutions, and software tools.

Healthcare: 17%. Includes specialized healthcare apps and administrative systems.

HR, Recruiting, and Benefits: 15%. Breaches exposed employee PII, which is valuable for fraud or espionage.

National Security: 11%. Breaches exposed sensitive hardware, intellectual property, or personnel.

Miscellaneous: 3%. These breaches did not fit any other categories.



The distribution of breach-enabling categories aligns with expectations. **Third-party technology products and services** consistently rank as the top sources of third-party risk, contributing to as much as **75% of breaches**, as noted in our global third-party breaches report. That report also highlights the **healthcare sector** as another significant contributor to third-party breaches, with its specialized products and services experiencing a higher breach rate than most other industries.

MOVEit File Transfer Software

The **MOVEit file transfer software** emerged as a notable contributor to third-party breaches in this sample. Two entries linked to MOVEit accounted for **6 breaches**, representing **17% of third-party breaches** and **10% of all breaches** in the sample. These breaches were tied to a mid-2023 campaign by **Cl0p ransomware operators,** who exploited a zero-day vulnerability in MOVEit (**CVE-2023-34362**). This campaign targeted organizations directly using the software as well as those indirectly exposed through their vendors. Due to the wide reach of this vulnerability, MOVEit has repeatedly surfaced as a top cause of third-party breaches across multiple industry-specific analyses.

HR, Recruiting, and Benefits

Breaches involving **outsourced HR, recruiting, and benefits services exposed employee personally identifiable information (PII).** This data is valuable for identity theft and fraud, as well as for foreign intelligence agencies seeking to recruit **human intelligence (HUMINT)** sources among federal contractors. These types of breaches accounted for a significant share of third-party incidents, underscoring the critical need for improved security in HR and benefits platforms.

National Security Context

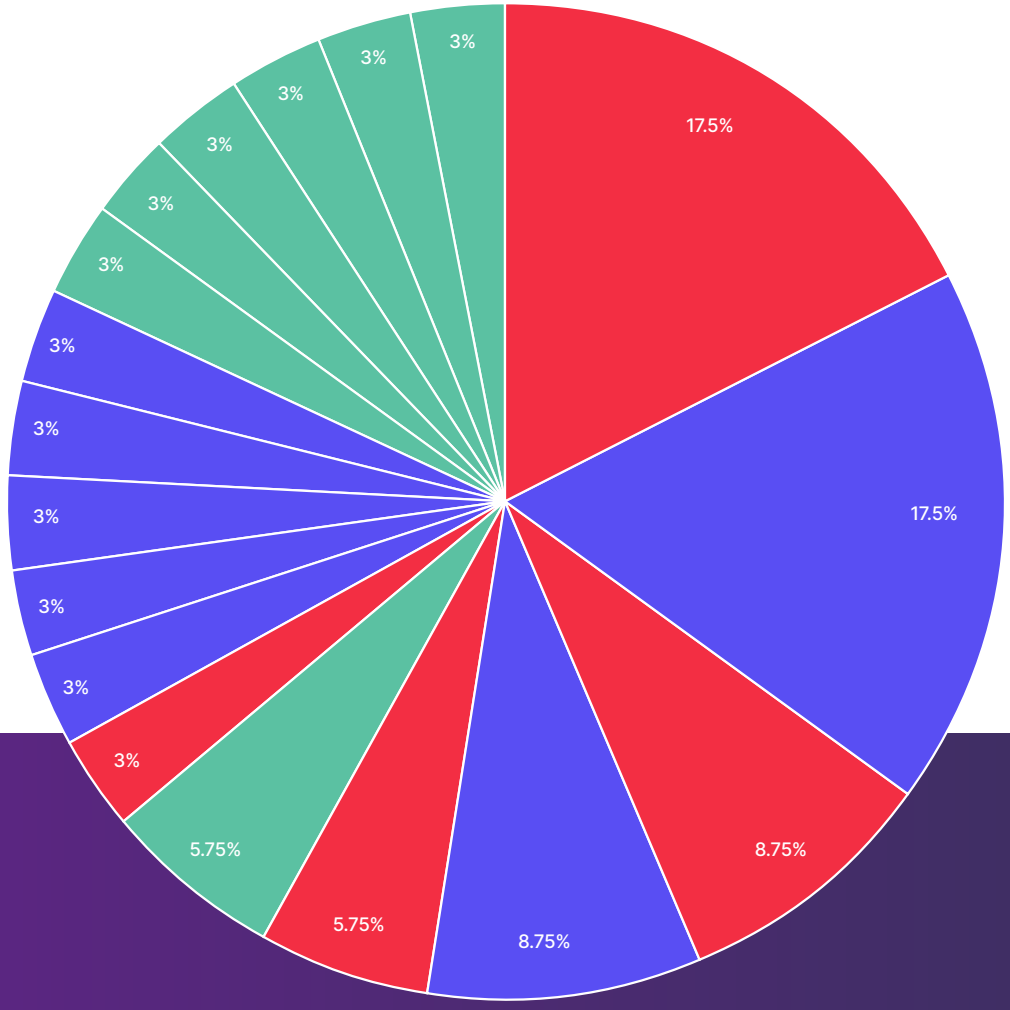
The relatively low presence of **U.S. national security** data in these breaches may seem unexpected. However, this aligns with findings that only a fraction of breaches directly impact USG operations. Many breaches involved contractor segments unrelated to federal contracts, such as commercial business areas. Additionally, air-gapped and segmented networks used by contractors likely protect sensitive national security systems, reducing the broader impact of breaches on the USG.

Threat Actor Attribution

Of the 60 breaches in our dataset, 34 were attributed to specific threat actors. These attributions include ransomware operators, state-sponsored groups, and other criminal or hacktivist entities. The breakdown of these actors is summarized in the following chart. For state-sponsored groups, the entries are consolidated by the sponsoring country, while criminal actors include usernames from underground forums or marketplaces where stolen data was disclosed or sold.

DISTRIBUTION OF ATTRIBUTABLE BREACHES BY THREAT ACTOR/STATE SPONSOR

- China: 6 breaches/17.5%
- Cl0p ransomware: 6 breaches/17.5%
- Russia: 3 breaches/8.75%
- LockBit ransomware: 3 breaches/8.75%
- North Korea: 2 breaches/5.75%
- "IntelBroker:" 2 breaches/5.75%
- Iran: 1 breach/3%
- BlackCat ransomware: 1 breach/3%
- Abyss ransomware: 1 breach/3%
- Lapsus$ ransomware: 1 breach/3%
- Trigona ransomware: 1 breach/3%
- PYSA ransomware: 1 breach/3%
- SiegedSec: 1 breach/3%
- "MajorNelson:" 1 breach/3%
- "Menelik:" 1 breac/3%
- "grep:" 1 breach/3%
- "0×3a0:" 1 breach/3%
- "133tfg:" 1 breach/3%



Categorization of Threat Actors

We grouped these 34 attributions into three main categories:

State-Sponsored Groups:

- Includes China, Russia, North Korea, and Iran.
- These actors were responsible for 12 breaches, making up 35% of all attributable breaches.

Ransomware Operators:

- Includes groups like Cl0p, LockBit, and BlackCat.
- Responsible for **14** breaches, accounting for **41.25%** of attributable incidents.

Miscellaneous Criminal and Hacktivist Actors:

- Includes individual forum actors and hacktivists like “IntelBroker” and SiegedSec.
- Accounted for **8 breaches,** or **23.75%** of the total.

Observations on Attribution

State-sponsored groups are often expected to dominate attacks on federal contractors due to their access to sensitive government data. However, in this dataset, their share was limited to **35%** of attributable breaches. Many contractors focus heavily on commercial clients alongside federal contracts, making them appealing targets for criminal actors who are less interested in government-specific data.

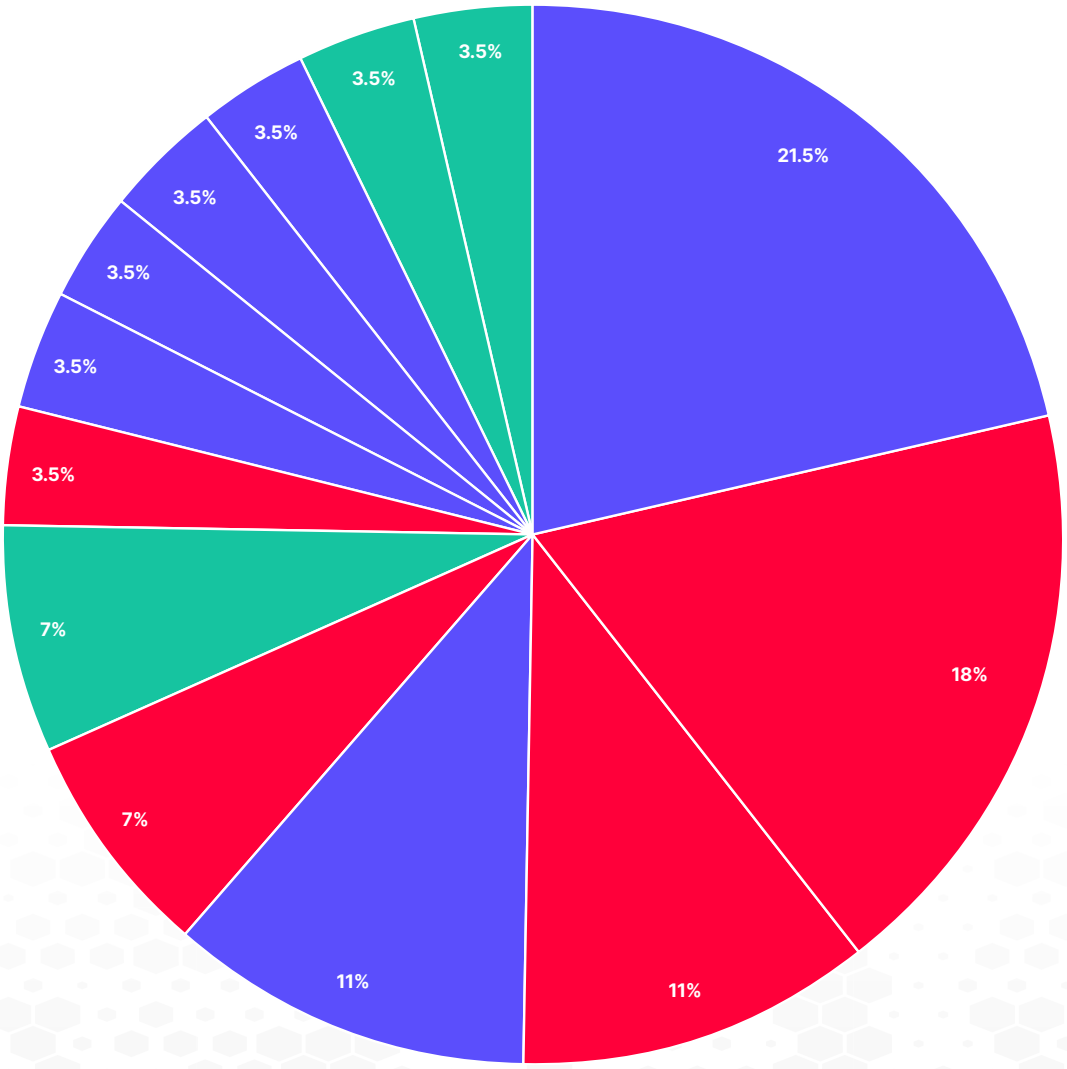
In fact, ransomware operators accounted for the largest share, responsible for **41.25% of breaches**. Groups like **Cl0p ransomware** and **LockBit** were as active as leading state-sponsors of cyber espionage like China and Russia. The **Cl0p ransomware group**, for example, tied with China for the top position, due to their high-profile exploitation of the MOVEit file transfer vulnerability in mid-2023. Similarly, LockBit was as prolific as Russian state-sponsored groups, reflecting the increasing sophistication of ransomware operations.

Attribution of Third-Party Breaches

Further analysis focused on third-party breaches linked to named actors. Of the **60 total breaches, 28 were both attributed to specific actors** and identified as third-party breaches. The breakdown is as follows:

DISTRIBUTION OF ATTRIBUTED THIRD-PARTY BREACHES BY THREAT ACTOR/NATION-STATE

- **Cl0p ransomware:** 6 breaches (21.5%)
- **China:** 5 breaches (18%)
- **Russia:** 3 breaches (11%)
- **LockBit ransomware:** 3 breaches (11%)
- **North Korea:** 2 breaches (7%)
- **"IntelBroker":** 2 breaches (7%)
- **Iran:** 1 breach (3.5%)
- **BlackCat ransomware:** 1 breach (3.5%)
- **Abyss ransomware:** 1 breach (3.5%)
- **Trigona ransomware:** 1 breach (3.5%)
- **Lapsus$ ransomware:** 1 breach (3.5%)
- **SiegedSec:** 1 breach (3.5%)
- **"133tfg":** 1 breach (3.5%)



Shifts in Threat Actor Patterns

Third-party breaches showed a shift in threat actor distribution. Both state-sponsored groups and ransomware operators had an increased presence:

State-sponsored third-party breaches rose to **39.5%** of the subset.

Ransomware groups accounted for **46.5%** of third-party breaches.

Miscellaneous criminals and hacktivists dropped to **14%**, reflecting their limited use of sophisticated third-party attack vectors.

This shift reflects the greater sophistication required to exploit third-party attack vectors. Less skilled criminals and hacktivists rarely use these methods. **Ransomware groups**, by contrast, invest heavily in advanced tools and strategies, making third-party vectors a cornerstone of their operations. **State-sponsored groups** go even further, leveraging extensive resources and specialized talent to execute highly targeted attacks.

One of the earliest examples of this tactic came from Chinese cyber espionage groups like **APT10**, which targeted Managed Service Providers (MSPs) to gain access to client systems, including U.S. federal agencies. Ransomware groups later adopted this approach. For instance, the **REvil group** exploited a vulnerability in Kaseya's Virtual Systems Administrator (VSA) software to infect MSP customers, causing widespread disruption.

These findings highlight the growing reliance of sophisticated actors on third-party breaches, underscoring the need for robust supply chain defenses.

Examples of Breaches

Breaches impacting U.S. Government (USG) contractors can expose sensitive national security data, disrupt operations, and compromise critical systems. The most alarming scenarios involve the theft of military or intelligence data, operational plans, or key infrastructure details. One such breach occurred in 2009 when Chinese cyber espionage actors compromised **Lockheed Martin**, exposing data on the **F-35 Joint Strike Fighter**. This breach exemplifies the risks federal contractors face and was among the nine breaches in our sample that directly impacted the USG.

Not all breaches with national security implications involve state-sponsored groups. In one case, **Abyss ransomware** attackers attempted to sell data on a contractor's support for Army satellite telecommunications systems. Criminal actors are keenly aware of the monetary value of national security data, often marketing stolen information to the highest bidder. For instance, a breach at General Electric revealed data tied to the **Defense Advanced Research Projects Agency (DARPA)**—another case among the nine that affected USG equities.

Some breaches stem from vulnerabilities in technology widely used by both the private sector and USG agencies. In one example, **Chinese cyber espionage group Storm-0558** exploited a vulnerability in **Microsoft Outlook**, compromising email systems used by USG agencies. These incidents underscore how common tools can become gateways for attacks on sensitive government systems.

The Role of Social Engineering

State-sponsored groups are often associated with sophisticated tactics, but some breaches rely on simpler methods. For example, the Iranian group **OilRig** used a fake Facebook persona to trick a **Deloitte** employee into opening a malicious file, compromising the contractor's systems. This breach exposed information on multiple clients, including USG agencies. It highlights that even straightforward social engineering can result in high-impact breaches.

Mundane Breaches with Significant Impact

Many breaches involve less dramatic targetsbut still yield sensitive data. For instance:

A breach at **Huntington Ingalls Industries**, a naval hardware manufacturer, exposed employee **personally identifiable information (PII)**. While the breach did not appear to compromise national security data, PII is valuable for identity theft and fraud. The PII of employees at a military hardware manufacturer would also be useful to foreign intelligence services seeking to recruit malicious insiders.

At **SAIC**, attackers accessed **security clearance applications (SF-86)**, exposing the personal details of individuals with classified access. This type of data could be of great use to foreign intelligence services seeking to recruit malicious insiders.

In many cases, such as the breach of DoD IT provider **Leidos,** the compromised documents are usually about the breached company itself, rather than any of its USG customers, or any sensitive products or services that they provide to the USG.

Third-Party and Supply Chain Breaches

Federal contractors often rely on their own vendors, making them vulnerable to third-party breaches:

LockBit ransomware operators disclosed technical data from NASA contractor **SpaceX** by compromising a Texas-based manufacturer in its supply chain.

In a remarkable example of cascading risk, a vulnerability in the **Confluence software suite** (CVE-2023-22515) led to a breach of **CGI Federal**. This incident exposed data from the **Government Accountability Office (GAO)** and its vendors, including **6,600 employees' PII**.

These examples underscore how third-party and even **fourth-party breaches** can reverberate across the federal supply chain, compromising sensitive USG data.

Recommendations

1. Extend DoD's Cyber Maturity Model Certification (CMMC)

The CMMC framework ensures contractors meet cybersecurity standards for sensitive DoD contracts. Contractors focused on national security scored highest in our sample, suggesting the model's effectiveness. Expanding CMMC to civilian agencies could address widespread vulnerabilities and enforce stricter security protocols across the federal supply chain.

2. Prioritize Third-Party Risk Management

While contractors undergo security reviews, current third-party risk management (TPRM) practices can be more targeted. Agencies should prioritize scenarios where contractor breaches are likely to expose USG equities. Narrower vetting parameters could help agencies focus on the most critical risks without overburdening review processes.

3. Expand to Fourth-Party Risk Management

Robust TPRM is only part of the solution. Many breaches stem from **fourth-party risks**—vendors and tools used by contractors themselves. Federal agencies should assess whether contractors have strong TPRM programs to reduce the likelihood of cascading vulnerabilities.

4. Require Disclosure of Breach Histories

Given the high breach rates in this sample, requiring contractors to disclose their breach histories could enhance transparency. While the SEC mandates such disclosures for publicly traded companies, privately owned contractors remain under less scrutiny. Breach history disclosures could be a useful addition to federal contractor vetting.

5. Focus on Specific Security Issues

Application Security, DNS Health, and Patching Cadence emerged as critical vulnerabilities in our analysis. Agencies should incorporate these factors into routine assessments. Public-facing websites and DNS records are good starting points for identifying potential issues.

6. Address Both Criminal and State-Sponsored Threats

Criminal groups, particularly ransomware operators, remain a major threat to federal contractors. While state-sponsored attacks garner attention, **41.25% of attributable breaches** in our sample were linked to ransomware groups. Federal contractors must enhance defenses against both types of attackers, recognizing that sensitive operations make them prime targets for diverse threats.

CONCLUSION

straightforward social engineering to cascading risks within supply chains. Strengthening cybersecurity across all levels of the federal supply chain is not only necessary but urgent. Addressing gaps in third and fourth-party risk management, requiring greater transparency, and expanding proven frameworks like CMMC will help secure the USG's most critical assets against evolving threats.

To learn more and create your free account, visit SecurityScorecard.com

ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io