REPORT

# 2025 SecurityScorecard Global Third-Party Breach Report

## From Ratings to Resilience

SecurityScorecard

# Modern cybersecurity isn't failing because organizations are ignoring threats—it's failing because they're looking in the wrong direction.

While security teams work to secure their own networks, attackers are already finding ways in through the back door—exploiting vendors, suppliers, and software providers to infiltrate organizations without ever touching their carefully monitored perimeters.

In 2024, at least 35.5% of all data breaches originated from third-party compromises, up 6.5% from the previous year. This number is likely an undercount, as many organizations may be unaware of or choose not to disclose the third-party origins of their breaches.

So while you're updating your firewall rules, somewhere in your supply chain a vendor might be inadvertently letting in the very attackers you've been working to keep out. And these attackers have figured out it's much easier to enter through a partner that already has trusted access.

## Why We're Here

At SecurityScorecard, we believe you can't fix what you can't see. That's why we analyzed 1,000 data breaches across all industries and geographic areas to uncover the true scale of third-party cyber risk. Our mission is to help you illuminate these blind spots and transform how you manage your extended security perimeter.

## What You'll Learn

- This report answers key questions including:
- How third-party risks have evolved since 2023
- Which industries and geographic areas experience the highest frequency of third-party breaches
- What specific vendor relationships are being exploited most frequently
- Which threat actors are behind these supply chain compromises
- The software vulnerabilities that continue to enable successful attacks
- How to move beyond traditional assessments to more effective security measures

**Bad actors aren't just breaking into homes anymore—they're breaking into the factories that make the locks for the doors.**

# Table of Contents

# Don’t let a third party reality check become checkmate

More than 1 in 3 breaches (35.5%) now come through third parties—attackers aren’t breaking in; they’re logging in with your partners’ credentials while you’re busy patching your own systems.

## Industries in the crosshairs

**Retail & Hospitality**
A staggering **52.4%** of all breaches come through third parties

**Critical Infrastructure**
Energy and utilities face a **46.7%** third-party breach rate

**Technology industries**
experience **disproportionately high rates** of third-party breaches relative to total breach volume

**Healthcare**
has a **large share** of third-party breaches due to high overall breach volume

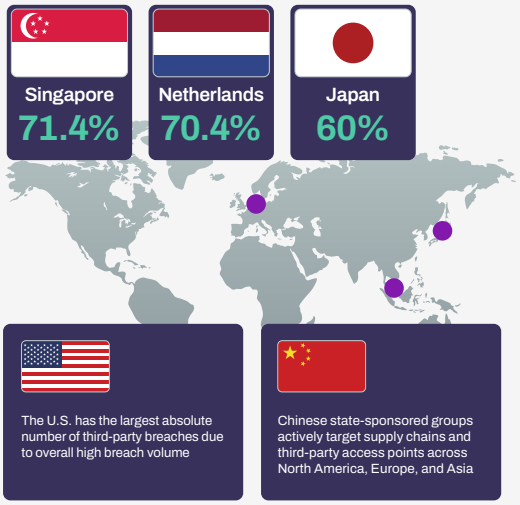
## The cascading impact

**4.5%** of breaches now extend to fourth parties—one breach triggers multiple organizational failures

Foreign subsidiaries are **2×** more likely to be breach sources than domestic ones

## Global vulnerability landscape

More affluent countries may have stronger security but also have higher third-party breach rates:




## The calculated attack strategy

- Ransomware Connection: **41.4%** of ransomware attacks now start through third parties
- The ransomware group **C10p** stands out as the **most prolific user** of third-party access vectors, as it did in last year’s report.
- Just two vulnerability exploits in file transfer software caused **63.5%** of all vulnerability-based breaches
- Software Supply Chain Under Siege: **File transfer** software vulnerabilities have become the **most common** attack vector for third-party breaches
- **State-sponsored** cyber espionage campaigns from China frequently leverage third-party access.

## The bottom line

Traditional security is looking in the wrong direction, leaving organizations vulnerable to attacks that bypass their own defenses entirely

Adversaries use third-party access vectors for scalability—compromising multiple organizations through a single vulnerable entry point

# The Data
## OSINT, Threat Intelligence & Underground Research

Unlike other reports that rely solely on self-reported data (we see you, survey-based studies), this study integrates real-world breach intelligence gathered by SecurityScorecard's STRIKE Threat Intelligence Unit. Most breaches in our sample were not third-party related—this was intentional to provide a broader comparison sample and identify ways in which third-party breaches differ from the general risk landscape.

**Our definition of a third-party breach includes:**

- **Lateral movement attacks** – When attackers use compromised access at a vendor, supplier, or partner to infiltrate the networks of their business-to-business (B2B) customers or other partners.
- **Vendor data breaches** – When data from one organization is compromised while in the custody of a vendor, supplier, or service provider.

Security teams can no longer afford to treat third-party security as a compliance checkbox. Traditional vendor risk assessments—conducted annually or quarterly—are too slow to detect active threats. While you're scheduling your next quarterly assessment, attackers are already three vendors deep into your supply chain.

This report will demonstrate why leading organizations are shifting from reactive third-party risk management to real-time supply chain threat detection. The future of cybersecurity depends on protecting your network and your entire ecosystem.

# Top Takeaways

## The Rising Tide of Third-Party Breaches

35.5% of all breaches in 2024 were third-party related, a 6.5% increase from 2023. This number is likely conservative, as many third-party breaches go unreported or are mistakenly assumed to be internal incidents. It's like playing "Spot the Breach Origin"—harder than you'd think and nobody wins.

## Industries at Highest Risk

Healthcare, Pharmaceuticals, and Biotechnology had the highest volume of third-party breaches. However, this is largely due to high overall breach numbers and strict U.S. breach disclosure requirements.

Retail, Hospitality, and Consumer Goods, along with Technology, Telecommunications, and Media, experienced the highest relative third-party breach rates. These industries had a higher proportion of third-party breaches compared to their total breach volume.

Energy, Utilities, and Critical Infrastructure had a disproportionately high rate of third-party breaches despite its smaller share of overall breaches. This aligns with prior research indicating that critical infrastructure is highly vulnerable to third-party risks.

## Geopolitical & Regional Trends

North America accounted for 59% of total breaches but only 53% of third-party breaches. The U.S. sees a high volume of breaches in general, but many of them are direct attacks, particularly in healthcare.

Europe, Northeast Asia, and Oceania exhibited higher relative rates of third-party breaches. Japan consistently records some of the highest third-party breach rates, while the Netherlands led in 2024 due to a single large breach at a customer communications firm that impacted multiple utilities and housing associations.

Chinese state-sponsored groups continue to use third-party attack vectors in supply chain compromises, particularly targeting Asian and Western organizations. The Philippines also had a surprisingly high number of breaches in our dataset, particularly third-party breaches, due to its importance as a target of Chinese cyber espionage.

## Attackers & Threat Vectors

Chinese cyber espionage actors frequently use third-party attack vectors, particularly in regional supply chain compromises.

The ransomware group C10p remains the most prolific third-party attacker, leveraging file transfer software vulnerabilities to breach multiple organizations at once.

RansomHub is emerging as the most dominant non-C10p ransomware group, likely filling the vacuum left by AlphV/BlackCat's disbanding and law enforcement actions against LockBit.

UNC5537's campaign against Snowflake cloud services significantly contributed to cloud platforms becoming the second most common third-party attack vector in 2024.

## The Role of Technology in Third-Party Breaches

46.75% of third-party breaches involved technology products and services, a significant drop from last year's 75%, signaling a diversification of attack surfaces.

File transfer software remained the top third-party breach enabler, with C10p exploiting vulnerabilities in Cleo software (CVE-2024-50623 & CVE-2024-55956) to launch large-scale attacks.

Cross-industry technology was four times more commonly exploited than industry-specific technology, reflecting the broad reach of supply chain risks. Despite this, products & services specific to Healthcare and Financial Services (both technical and non-technical) together accounted for 27.5% of third-party breach origins, nearly the same as last year.

## Third-Party Breaches & Ransomware: A Growing Nexus

41.4% of ransomware and extortion incidents had a third-party breach component, indicating an increasing reliance on supply chain infiltration.

C10p's large-scale exploitation of Cleo vulnerabilities dwarfed all other known third-party exploits, reinforcing its reputation as the most prolific third-party attacker.

## The Affluence Factor

A correlation is emerging between economic development and third-party breach frequency. Wealthier nations experience more third-party attacks due to their interconnected supply chains and higher security standards, which drive attackers toward indirect access points.

Affluent countries such as Singapore, the Netherlands, and Japan had among the highest third-party breach rates. In contrast, China, Brazil, and Russia—despite high overall breach numbers—saw fewer third-party breaches, likely due to different attack patterns and fewer business-to-business dependencies.

# Third-Party vs. Fourth-Party Breach Trends

## The Expanding Risk Chain

Supply chain attacks are increasing as hackers exploit the weakest links in security. As organizations strengthen their internal defenses, attackers bypass them by targeting less secure vendors, suppliers, and service providers. Our analysis of 1,000 breaches highlights the growing risks in third-party and fourth-party breaches.

## Third-Party Breaches Are Rising Fast

- 35.5% of breaches (355 cases) involved a third-party nexus, up from 29% last year, marking a 6.5% increase.
- Attackers are increasingly exploiting third-party access to evade strong internal security measures.
- The rise in outsourcing, interdependence, and cloud reliance has created more opportunities for attackers to leverage third-party weaknesses.

## Fourth-Party Breaches Create Cascading Failures

- 45 breaches extended beyond third parties to involve yet another organization in the supply chain.
- These fourth-party breaches accounted for 4.5% of all breaches and 12.7% of third-party breaches.
- The interconnected nature of modern business ecosystems means that a single compromise can trigger widespread disruptions across multiple organizations.

## The Hidden Iceberg: Underreported Third-Party Risks

- The true scale of third-party and fourth-party breaches is likely higher than reported. For example a global food retailer reports that 67% of breaches were caused by third-parties.
- Many breach reports lack details on the attack vectors, tactics, and stolen data, making it difficult to identify third-party involvement.
- The complexity of modern supply chains means that many third-party connections remain invisible until they are exploited.

As businesses become more interconnected, the attack surface continues to expand. In the next section, we examine which industries, regions, and countries are facing the greatest third-party risks.

# Distribution of Third-Party Breaches by Industry

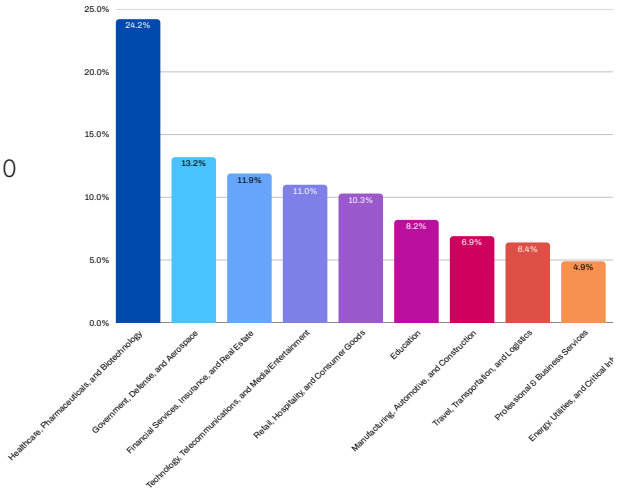
## Understanding the Three Key Metrics

We examined third-party breach risk through three different but complementary lenses. Here's what each measurement tells us:

## 1. Total Breach Count by Industry

This shows which industries experience the most breaches overall:

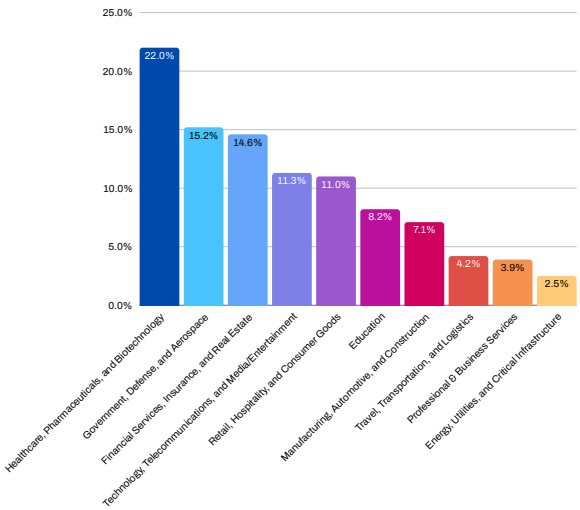
1. Healthcare, Pharmaceuticals, and Biotechnology: 242 breaches (24.2%)
2. Government, Defense, and Aerospace: 132 breaches (13.2%)
3. Financial Services, Insurance, and Real Estate: 119 breaches (11.9%)
4. Technology, Telecommunications, and Media/Entertainment: 110 breaches (11%)
5. Retail, Hospitality, and Consumer Goods: 103 breaches (10.3%)
6. Education: 82 breaches (8.2%)
7. Manufacturing, Automotive, and Construction: 69 breaches (6.9%)
8. Travel, Transportation, and Logistics: 64 breaches (6.4%)
9. Professional & Business Services: 49 breaches (4.9%)
10. Energy, Utilities, and Critical Infrastructure: 30 breaches (3%)




## 2. Third-Party Breach Count by Industry

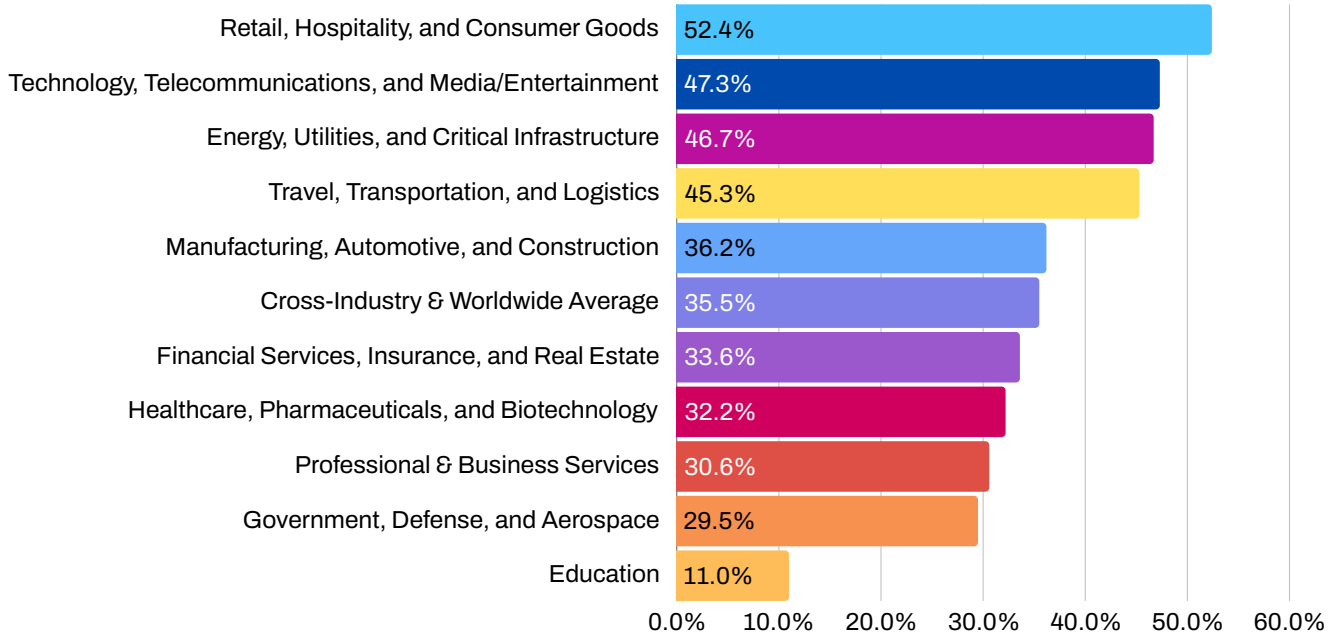
This shows which industries experience the most breaches specifically through third parties:

1. Healthcare, Pharmaceuticals, and Biotechnology: 78 breaches (22%)
2. Retail, Hospitality, and Consumer Goods: 54 breaches (15.2%)
3. Technology, Telecommunications, and Media/Entertainment: 52 breaches (14.6%)
4. Financial Services, Insurance, and Real Estate: 40 breaches (11.3%)
5. Government, Defense, and Aerospace: 39 breaches (11%)
6. Travel, Transportation, and Logistics: 29 breaches (8.2%)
7. Manufacturing, Automotive, and Construction: 25 breaches (7.1%)
8. Professional & Business Services: 15 breaches (4.2%)
9. Energy, Utilities, and Critical Infrastructure: 14 breaches (3.9%)
10. Education: 9 breaches (2.5%)



## 3. Third-Party Breach Rate Within Each Industry

This reveals what percentage of each industry's breaches come through third parties:




### Why These Distinctions Matter

- Healthcare has the most third-party breaches by count (78), but a below-average rate (32.2%)
- Retail has fewer total breaches than Healthcare (103 vs. 242), but over half (52.4%) involve third parties
- Education has both few third-party breaches (9) and the lowest rate (11%)

### The Bottom Line

Looking at just breach counts can be misleading. What matters is understanding both total breaches and the percentage coming through third parties:

- Retail leads with over half (52.4%) of breaches from third parties
- Healthcare has the most breaches overall but a below-average third-party rate (32.2%)
- All industries should prioritize supply chain security, but those with high third-party rates face proportionally greater risk through their vendor ecosystem

ATTACK PATTERNS

# Healthcare Tops Breaches in General

Healthcare, Pharmaceuticals, and Biotechnology dominates the breach landscape with the highest number of incidents in both overall breaches and third-party breaches. However, a closer look reveals an important pattern in how these breaches occur:

## Key Statistics Explained:

- Healthcare accounts for 78 third-party breaches (22% of all third-party breaches) - this is the highest raw number among all industries
- However, looking at the proportion within healthcare itself, only 32.2% of its breaches involve third parties (compared to 35.5% across all industries)
- In other words: Out of healthcare's 242 total breaches, only 78 (32.2%) came through third parties
- This means healthcare faces more direct attacks than attacks through its vendor ecosystem compared to the cross-industry average

## Why This Matters

Healthcare suffers from the most breaches overall (242 incidents, 24.2% of all breaches), but a smaller percentage of these breaches involve third parties than the cross-industry average. This isn't due to greater resilience against third-party attacks, but rather reflects the sheer volume of direct attacks targeting healthcare organizations.

## Multiple Factors Drive Healthcare's High Breach Volume

Several key factors contribute to healthcare's position at the top of the breach statistics:

- Perceived weaker security makes healthcare a soft target for attackers
- Lower downtime tolerance makes healthcare particularly vulnerable to ransomware attacks
- Healthcare records contain rich personal data, making them highly valuable to attackers
- U.S. breach disclosure laws may artificially inflate healthcare's breach numbers compared to other sectors

## The Direct Attack Pattern

The data suggests that attackers often find direct routes into healthcare systems more viable than going through their suppliers or partners. This observed pattern indicates that when a target's direct defenses present sufficient vulnerabilities, attackers may not need to resort to the often more complex approach of compromising third-party relationships.

The prevalence of straightforward patient data breaches from U.S. providers with no third-party involvement supports this pattern, suggesting attackers are finding direct routes into healthcare systems without needing to leverage vendor relationships.

# Retail & Hospitality and Technology & Telecommunications Lead in Third-Party Breach Exposure

Two industries stand out in our analysis with high third-party breach rates and notable increases in their representation among third-party incidents:

## Retail & Hospitality: The Most Vulnerable Industry

- The only industry with a third-party breach majority: 52.4% of all its breaches involve third parties
- Ranks fifth in overall breaches but jumps to second place for third-party breaches
- Substantial increase in share from 10.3% of all breaches to 15.2% of third-party breaches

## Technology & Telecommunications: Close Second

- 47.3% of breaches involve third parties
- Moves from fourth place overall to third place for third-party breaches
- Share increases from 11% of all breaches to 14.6% of third-party breaches

## The Big Three Dominate

- Together with Healthcare, these three industries account for 51.8% of all third-party breaches
- This distribution is consistent with our previous findings
- Last year's report highlighted Healthcare and Technology as top third-party targets
- Our Japan-specific study (the country with the highest third-party breach rate) also identified Technology and Retail & Hospitality as particularly vulnerable within that market

## Why Retail & Hospitality Is So Vulnerable

- Historically targeted for payment card data
- Card breaches inherently involve third parties (banks that issue cards and bear fraud-related losses)
- Modern e-commerce platforms rely heavily on third-party vendors:
  - Hosting companies
  - Software developers
  - Specialized e-commerce service providers
- Compromises at technology vendors can create cascading breaches (fourth-party)

## The Technology Sector's Unique Risk Profile

- SecurityScorecard research confirms technology companies face among the highest third-party risks
- They occupy a dual position: both enabling third-party attacks on customers and suffering attacks via their own vendors
- Typically maintain larger, more complex attack surfaces
- This complexity creates additional challenges for both attackers and defenders

# Energy and Transportation Sectors Show Alarming Third-Party Breach Rates

For each of the 150 insurance companies, we identified their lowest sub-scoring security factor out of 10 possible categories. These factors contribute to their overall scores.

## Energy, Utilities, and Critical Infrastructure

### HIDDEN HIGH RISK

- Third-highest frequency of third-party breaches at 46.7% (14 of 30 breaches)
- Represents just 3% of all breaches but faces disproportionate third-party risk
- Consistent with SecurityScorecard's previous analysis of the U.S. energy supply chain
- U.S. energy sector showed similar patterns with 45% of breaches having third-party connections
- Global energy sector appears to follow similar vulnerability patterns as observed in the U.S.

## Travel, Transportation, and Logistics

### FOURTH MOST VULNERABLE

- Fourth-highest third-party breach rate at 45.3%
- Share of third-party breaches (8.2%) exceeds its share of total breaches (6.4%)
- Elevated risk largely attributed to a targeted campaign by a prolific threat actor
- The C10p ransomware group specifically targeted this industry
- C10p's history of exploiting software vulnerabilities aligns with third-party attack vectors
- This concentrated campaign was significant enough to skew industry-wide statistics

**More details on this specific campaign are covered in later sections of the report**

These findings highlight how even industries with relatively fewer total breaches can face significant supply chain security challenges, with nearly half of all incidents originating through third parties.

# Third-Party Breach Hotspots

## Supply Chain Risk Varies Dramatically by Geography

Our analysis of 355 third-party breaches reveals notable regional and national patterns in digital supply chain vulnerability.

## Regional Risk Profile

### NEGATIVE SCORE IMPACT FOR EACH COMPANY

**Regional Breakdown Comparison:**

| Region | All Breaches | Third-Party Breaches | Third-Party Rate |
|---|---|---|---|
| North America | 59% | 53% (188 breaches) | 31.9% |
| Northeast Asia | 11.6% | 17.7% (63 breaches) | 54.3% |
| Europe | 13.4% | 14.6% (52 breaches) | 38.8% |
| South & Southeast Asia | 6.8% | 6.8% (24 breaches) | 35.3% |
| Oceania | 3.7% | 4.5% (16 breaches) | 43.2% |
| Middle East & Africa | 2.1% | 1.7% (6 breaches) | 28.6% |
| Latin America & Caribbean | 1.8% | 1.1% (4 breaches) | 22.2% |
| Former Soviet Union | 1.6% | 0.6% (2 breaches) | 12.5% |
| Worldwide Average | 100% | 100% | 35.5% |

## Key Regional Insights

- While North America dominates total breach volumes, its third-party breach rate (31.9%) falls below the global average
- Northeast Asia stands as the only region where more than half of all breaches (54.3%) involve third parties
- Three regions—Northeast Asia, Oceania, and Europe—show both higher third-party breach rates and increased representation in the third-party breach subset

## Nation-Level Analysis

### UNEXPECTED LEADERS IN SUPPLY CHAIN RISK

**Country Distribution Comparison:**

| Country | Share of All Breaches | Share of Third-Party Breaches | Third-Party Rate |
|---|---|---|---|
| United States | 56% | 48.7% | 30.9% |
| Japan | 9.4% | 15.8% | 60.0% |
| Netherlands | 2.7% | 5.4% | 70.4% |
| United Kingdom | 4.3% | 4.5% | 37.2% |
| Australia | 3.2% | 4.5% | 50.0% |
| Canada | 3.0% | 3.7% | 43.3% |
| Philippines | 2.9% | 2.5% | 31.0% |
| Germany | 1.7% | 2.3% | 47.1% |
| India | 2.0% | 2.0% | 35.0% |
| Singapore | <1% | 1.4% | 71.4% |
| Taiwan | <1% | 1.1% | 57.1% |
| Global Average | | | 35.5% |

## The Concentration Effect

- While 12 countries accounted for 88.4% of all breaches, just 11 countries account for 91.9% of all third-party breaches globally
- Country-level third-party breach rates show even more dramatic variation than regional rates
- Smaller but economically advanced nations face disproportionately high third-party breach risks

## Notable National Findings

- Singapore: Highest third-party breach rate (71.4%) despite relatively few total breaches
- Netherlands: Second highest rate (70.4%), influenced by a major breach at a communications firm affecting multiple utilities
- Japan: Third highest rate (60%), continuing a pattern identified in previous reports
- Taiwan: 57.1% third-party breach rate despite few total breaches
- Singapore's high rate (71.4%) appears in our data alongside documented Chinese cyber operations

# Geopolitical Patterns

## Supply Chain Attack Trends

### The East Asian Trends

- Japan's persistently high third-party breach rate (60%) relates to two factors:
- Complex subsidiary structures of Japanese multinational corporations
- Targeted Chinese state-sponsored attacks using third-party vectors
- Taiwan's high third-party breach rate (57.1%) correlates with its status as a focus of Chinese cyber espionage
- Singapore's high rate (71.4%) appears in our data alongside documented Chinese cyber operations

# The China Connection

Singapore made our top countries list for third-party breaches while missing the general breach list entirely. With its significant overseas Chinese population and strategic position in China's economic and naval power projection, it's a prime target. Though we should note Singapore's smaller breach sample size might be inflating that eye-popping 71.4% rate.

The Philippines stands out as the oddball on both lists—seventh for general breaches and eighth for third-party breaches. Unlike its list companions, it's neither a major geopolitical power nor an economic heavyweight. This developing nation earned its spot through Chinese cyber campaigns tied to maritime territorial disputes. For example, Chinese state-sponsored actors compromised a cloud provider to access six Filipino government domains, including the Coast Guard and National Coastal Watch System.

Australia faces similar Chinese cyber attention, but that doesn't fully explain Oceania's elevated third-party breach numbers. Similarly, the U.K. and Germany's higher breach rates don't account for Europe's above-average third-party statistics. The Netherlands, however, gives us a clearer picture with its 5.4% share and 70.4% third-party breach rate (highest in our sample). One large-scale breach at a Dutch customer communications firm cascaded through Dutch water companies/authorities, utilities, and housing associations.

# North American Nuances

The U.S. posts a lower third-party breach rate (30.9%)—4.6% below the global average. This stems primarily from America's high volume of direct healthcare breaches and stricter disclosure laws, which inflate the overall breach count and make third-party incidents appear less significant by comparison. The U.S. breach volume effectively dilutes global third-party statistics, masking substantive supply chain issues.

Canada's elevated third-party breach profile lacks a single explanation. We theorize that the higher third-party breach rates across Canada, Australia, and major European economies may simply represent the "new normal" for Western democracies with advanced economies.

# Research Reality Check

- We recognize potential sampling bias toward English-speaking countries, especially the U.S., and have worked to counter this by incorporating more non-English sources and broadening international coverage.
- Singapore's impressive-looking 71.4% third-party breach rate deserves some skepticism given its smaller sample size—a reminder that percentages without context can mislead even seasoned analysts.

# The Wealth Effect

## Economic Prosperity Correlates with Third-Party Breach Risk

A counterintuitive pattern – wealthier nations face significantly higher third-party breach risks. This finding builds on our previous research establishing that organizations in more affluent countries typically have stronger security postures.

## The Wealth-Risk Paradox

Previous SecurityScorecard research established that organizations in wealthier countries generally maintain stronger security than those in developing economies. Paradoxically, our current analysis suggests these same affluent nations face disproportionately high third-party breach risks:

- Less affluent economies show declining representation in third-party breaches:
  - China, Brazil, and Russia appear among countries with the highest shares of breaches overall
  - Yet all three disappear from the list of countries with the highest shares of third-party breaches
- Affluent economies show increased representation in third-party breaches:
  - The much smaller but more affluent "Asian Tigers" of Taiwan and Singapore replace those less affluent nations on the third-party breach leaderboard
  - Nearly all countries with the largest shares of third-party breaches are economically advanced nations

## The Exceptions That Prove the Rule

Only three countries on our third-party breach leaderboard show below-average third-party breach rates:

- India: Its position is notable given:
  - Large economy and significant global market presence
  - English language usage
  - Key role in global supply chains
- Philippines: Its position in the data shows:
  - Presence of Chinese cyber operations
  - Campaigns targeting government agencies due to maritime territorial disputes
- United States: The only wealthy nation with below-average third-party breach rates:
  - Unique healthcare system producing numerous direct breaches
  - Large volume of breaches diluting the proportion of third-party incidents

## Why Wealthy Nations Face Higher Third-Party Risks

Two key factors explain why economic prosperity correlates with increased third-party breach risk:

- The Security Bypass Effect:
  - Organizations in affluent economies invest more in security
  - Attackers respond by seeking third-party vectors to circumvent stronger defenses
  - This creates a "path of least resistance" through supply chains
- The Complexity Multiplier:
  - Advanced economies feature more extensive:
    - Outsourcing relationships
    - Business interdependencies
    - Digital supply chains
  - Each connection represents a potential attack vector
  - Greater complexity increases the likelihood that breaches will cascade to partners

This correlation between wealth and third-party risk suggests organizations in advanced economies should place particular emphasis on their supply chain security programs.

# Products and Services at the Center of Supply Chain Risk

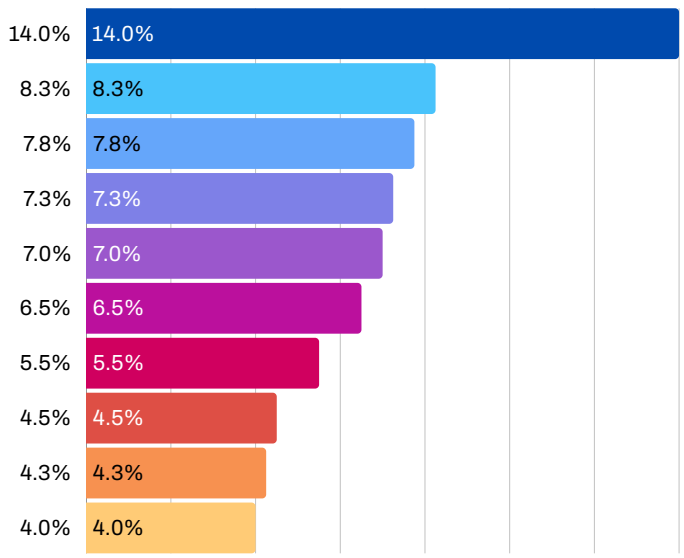
Third-party breach vectors tell a clear story. Looking across 400 relationships involved in supply chain attacks (355 third-party relationships and 45 fourth-party relationships), we can see which products and services attackers prefer to target:

## Breach Enablers by Major Category

| Category | Count | Percentage |
|---|---|---|
| Cross-Industry Software & IT | 150 | 37.5% |
| Industry-Specific Services (Non-technical) | 88 | 22.0% |
| Cross-Industry Services (Non-technical) | 52 | 13.0% |
| Subsidiaries & Acquisitions | 47 | 11.75% |
| Industry-Specific Software & IT | 37 | 9.25% |
| Other | 26 | 6.5% |

## The Top 10 Sources or Enablers of Third-Party Breaches

1. File transfer software: 56 breaches (14%)
2. Cloud products & services: 33 breaches (8.25%)
3. Foreign subsidiaries & acquisitions: 31 breaches (7.75%)
4. Payment card data breach: 29 breaches (7.25%)**
5. Pharmaceutical distribution & clinical trial support: 28 breaches (7%)*
6. Unspecified vendors: 26 breaches (6.5%)
7. Customer Relationship Management (CRM) & communications services: 22 breaches (5.5%)
8. Unnamed software & IT products & services: 18 breaches (4.5%)
9. Healthcare administrative and management services: 17 breaches (4.25%)*
10. Domestic subsidiaries & acquisitions: 16 breaches (4%)




*Specific to Healthcare **Specific to Financial Services

# Industry-Specific Third-Party Attack Vectors

### Healthcare-Specific Vectors (63 breaches, 15.75%):

- Pharmaceutical distribution & clinical trial support: 28 breaches (7%)
- Healthcare administrative and management services: 17 breaches (4.25%)
- Healthcare software, mobile apps, and telehealth services: 8 breaches (2%)
- Healthcare revenue cycle management, medical billing, and debt collection: 6 breaches (1.5%)
- Diagnostic lab testing and other specialized clinical services: 4 breaches (1%)

### Financial Services-Specific Vectors (47 breaches, 11.75%):

- Payment card data breach: 29 breaches (7.25%)
- Financial technology (FINTECH) & cryptocurrency infrastructure: 7 breaches (1.75%)
- Specialized insurance software & services: 7 breaches (1.75%)
- Payment processing and Automated Clearing Houses (ACHs): 4 breaches (1%)

### Additional Significant Breach Vectors

- Miscellaneous cross-industry software & IT: 14 breaches (3.5%)
- Miscellaneous industry-specific software & IT: 10 breaches (2.5%)
- Social media: 7 breaches (1.75%)
- Professional services: 7 breaches (1.75%)
- Call center operations: 6 breaches (1.5%)
- Telecommunications services: 6 breaches (1.5%)
- VPN software: 6 breaches (1.5%)
- Payroll & Human Resources (HR) products & services: 6 breaches (1.5%)
- Shipping, trucking, aviation, and other logistics: 6 breaches (1.5%)
- Cyber security products & services: 5 breaches (1.25%)
- Email, collaboration, and communication software: 5 breaches (1.25%)
- Software supply chain & development support: 5 breaches (1.25%)
- Consulting, advisory, and risk management: 5 breaches (1.25%)

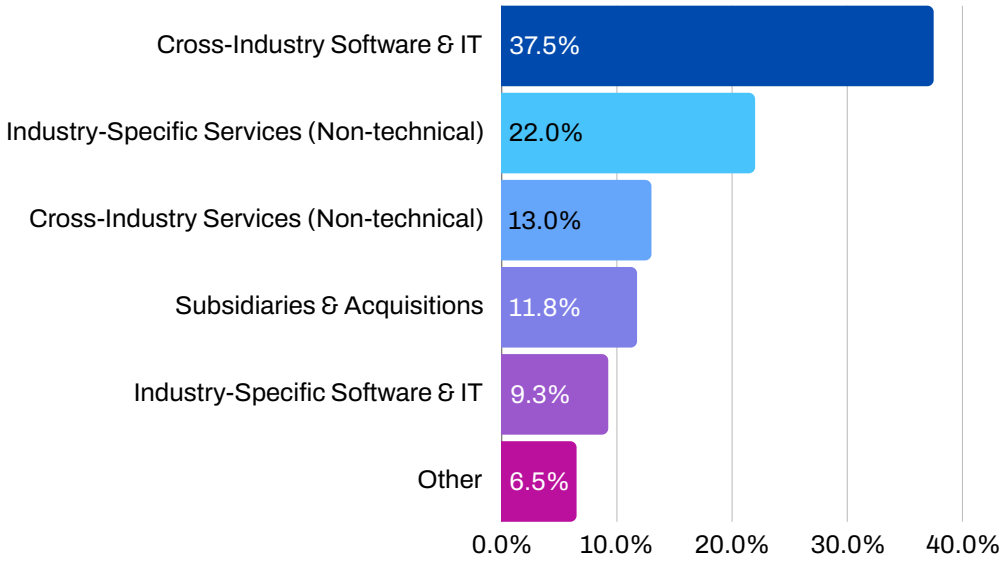
# Third-Party Breach Enablers

## Analysis Reveals Diverse Risk Landscape

Dissecting 400 connections (355 third-party and 45 fourth-party breaches) reveals which products and services attackers favor as their supply chain entry points. The data paints a clear picture of risk—technology remains significant but isn't the only vulnerability in today's ecosystem.

## Frequency of Breaches

The study categorized the products and services that enabled breaches into six broader categories:



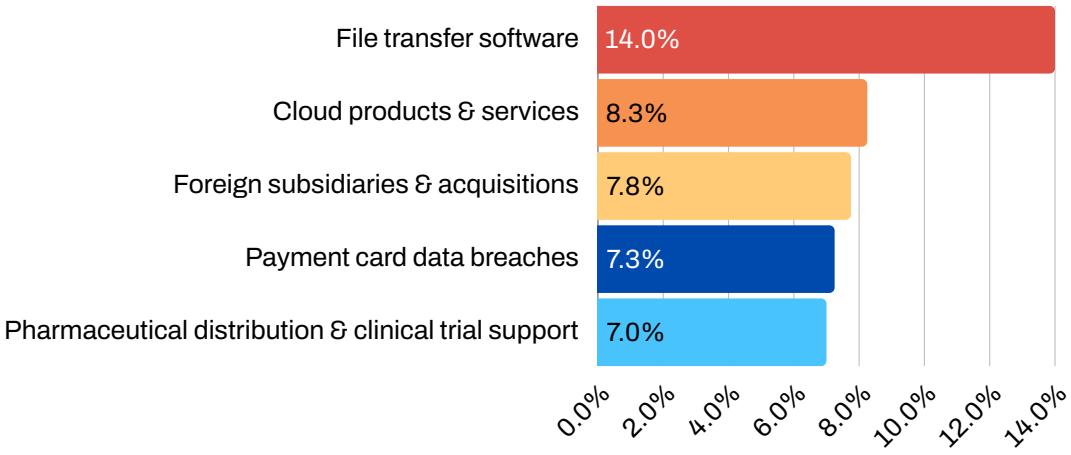

While technology products and services (combining Cross-Industry and Industry-Specific Software & IT) enabled 46.75% of third-party relationships involved in breaches, over half of the breaches (53.25%) stemmed from non-technology sources, highlighting the diverse nature of third-party risk.

## Technology's Role in Context

Previous SecurityScorecard findings suggested technology vendors were involved in approximately 75% of third-party breaches. Our current finding of 46.75% represents a notable difference, though direct year-over-year comparisons should be approached with caution due to differences in data samples and methodology.

## Specific Attack Vectors Across Categories

Key individual items that enabled breaches include:




This diversity of attack vectors spans both technology and non-technology categories, demonstrating the complex nature of the supply chain risk landscape.

## Emerging Patterns in Recent Studies

This broader distribution of third-party breach enablers, with a higher proportion of non-technical enablers, appears consistent with several recent SecurityScorecard studies, though more research is needed before confirming a definitive trend:

- Japan-specific analysis: 58% technology-enabled third-party breaches
- Global insurance industry study: 50% technology-enabled breaches
  - Cross-industry offerings: 37%
  - Insurance-specific offerings: 13%
- U.S. federal contractors analysis: 54% technology-enabled breaches

## Implications for Organizations

The findings suggest that while technology vendors remain the single largest category of third-party breach enablers, organizations face a broader range of potential risk vectors than previously emphasized.

This may indicate that as security measures around technology vendors mature, organizations should ensure their third-party risk management programs extend beyond traditional technology vendors to include the full spectrum of business relationships, including non-technical service providers, subsidiaries, and supply chain partners.

# Healthcare and Financial Services

## Industry-Specific Relationships Drive Unique Risks

Despite having below-average third-party breach rates, Healthcare and Financial Services account for a disproportionate share of industry-specific relationships involved in breaches. This paradox reveals important insights about how supply chain risk manifests differently across industries.

### The 27.5% Factor: Consistency Across Years

- Healthcare and Financial Services relationships involved in breaches: 27.5%
- Healthcare-specific relationships: 15.75%
- Financial Services-specific relationships: 11.75%
- Virtually unchanged from last year's findings: 28%
- Only industries besides Technology with multiple industry-specific relationship categories as breach vectors

### Understanding the Paradox

The significant representation of Healthcare and Financial Services in third-party breaches presents a contradiction:

**Both industries have below-average third-party breach rates:**

- Financial Services: 33.6%
- Healthcare: 32.2%
- Cross-industry average: 35.5%

Yet they dominate industry-specific relationship categories.

**This contradiction likely stems from:**

- High targeting levels making even below-average rates yield significant breach volumes
- The sheer volume of Healthcare breaches overall (24.2% of all breaches)
- Complex ecosystems with numerous specialized vendor relationships

### The Technical vs. Non-Technical Divide

Industry-specific relationships show dramatically different breach risk profiles across sectors:

**Technology products & services:**

- General cross-industry technology: 37.5% of breach relationships
- Industry-specific technology: 9.25% of breach relationships
- Ratio: Cross-industry is 4× more common than industry-specific

**Non-technical products & services:**

- Industry-specific non-technical services: 22% of breach relationships
- General cross-industry services: 13% of breach relationships
- Ratio: Industry-specific is nearly 2× more common than cross-industry

This reversal suggests that while cross-industry technology poses broad risk across sectors, the specialized non-technical relationships in Healthcare and Financial Services represent a unique vulnerability not shared by other industries.

Organizations in these sectors should ensure their third-party risk management programs account for both technology vendors and the specialized non-technical service providers unique to their industry.

# Subsidiaries & Acquisitions: The Hidden Third-Party Risk Within Your Own Organization

A notable source of third-party risk comes not from external vendors but from within an organization's own corporate family. The risk from subsidiaries and acquired companies represents a blind spot in many security programs.

## A Significant Global Risk Factor

- Subsidiaries and acquisitions account for 11.75% of third-party breaches globally
  - Foreign subsidiaries & acquisitions: 7.75% of breach relationships
  - Domestic subsidiaries & acquisitions: 4% of breach relationships
- While subsidiaries and acquisitions are a third-party risk globally, they are particularly prominent in Japan:
  - Japan study: 33% of third-party breaches
  - Global study: 11.75% of third-party breaches
- Examples identified across the U.S. and Europe demonstrate this is a widespread phenomenon

## Cross-Border Risk Comparison

Similar to our Japan findings, foreign entities appear more frequently in breach data than domestic ones:

- Japan study: Foreign subsidiaries were identified in breach relationships more frequently than domestic ones
- Global study: Foreign subsidiaries (7.75%) appeared nearly twice as frequently as domestic subsidiaries (4%) in breach relationships

## Why Subsidiaries and Acquisitions Create Unique Risks

The presence of subsidiaries and acquisitions in breach data, particularly foreign ones, may stem from multiple factors:

**Communication challenges:**

- Language barriers
- Time zone differences
- Varying cultural expectations around performance and communication
- Differing regulatory requirements

**Integration complexities:**

Security policies may not be fully implemented across acquired entities

- Security controls and monitoring may be inconsistent
- Technology stacks often remain disconnected for extended periods
- Inherited vulnerabilities may exist in acquired companies before the transaction

This analysis underscores that subsidiaries and acquisitions, while often considered internal to an organization, introduce third-party risk factors that merit attention within security programs.

# File Transfer Software

## The Leading Third-Party Risk Vector

File transfer software remains the most exploited third-party access point, though its prevalence has declined from 26% to 14% of third-party breach relationship

## The C10p Factor

C10p dominated this vector through two major campaigns:

**2023 MOVEit Campaign:**

- Exploited CVE-2023-34362
- Caused cascading breaches affecting hundreds or thousands of organizations

**2024 Cleo Campaign:**

- Exploited zero-day vulnerability CVE-2024-55956
- Leveraged insufficient patching of related CVE-2024-50623
- Targeted three Cleo products: Harmony, VLTrader, and Lexicom
- Compromised dozens of companies

## Strategic Targeting Pattern

C10p's 2024 campaign showed a clear focus on disrupting supply chains:

- One-third of targets were in Travel, Transportation, and Logistics or had roles in consumer supply chains
- Specifically targeted U.S. and Canadian trucking companies
- Targeted wholesale/retail distributors of food and consumer goods
- Claimed attack on Blue Yonder (supply chain software vendor) disrupted operations for Starbucks and supermarket chains

This pattern reveals a deliberate strategy to maximize economic impact through targeted supply chain disruption rather than random opportunistic attacks.

# Threat Actors

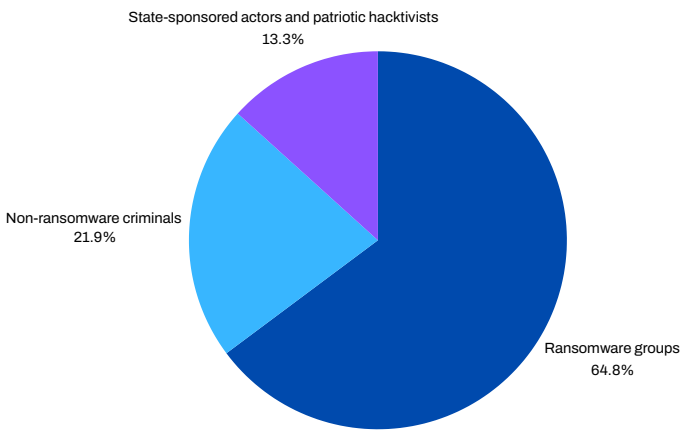
## Who's Behind the Breaches?

Looking at 315 attributable breaches reveals which threat actors caused the most incidents, especially those exploiting third-party access points

## Breach Attribution Landscape

### Distribution by Threat Actor Type

- Ransomware groups: 204 breaches (64.8%)
- Non-ransomware criminals and non-patriotic hacktivists: 69 breaches (21.9%)
- State-sponsored actors and patriotic hacktivists: 42 breaches (13.3%)




### Top Individual Threat Actors

1. C10p ransomware: 54 breaches (17%)
2. Miscellaneous criminals and hacktivists: 43 breaches (13.7%)
3. Miscellaneous ransomware operators: 29 breaches (9.2%)
4. LockBit ransomware: 26 breaches (8.2%)
5. China (state-sponsored): 20 breaches (6.3%)
6. RansomHub ransomware: 15 breaches (4.8%)
7. IntelBroker & Sanggiero: 13 breaches (4%)
8. Russia (state-sponsored): 10 breaches (3.2%)
9. BlackSuit ransomware: 10 breaches (3.2%)
10. UNC5537: 9 breaches (2.9%)
11. Akira ransomware: 9 breaches (2.9%)
12. Medusa ransomware: 8 breaches (2.5%)
13. Hunters International ransomware: 8 breaches (2.5%)
14. INC Ransom ransomware: 7 breaches (2.2%)
15. Black Basta ransomware: 7 breaches (2.2%)
16. Rhysida ransomware: 6 breaches (1.9%)
17. 8Base ransomware: 6 breaches (1.9%)
18. Ukraine (state-sponsored): 5 breaches (1.6%)
19. AlphV/BlackCat ransomware: 5 breaches (1.6%)
20. Play ransomware: 4 breaches (1.3%)
21. BianLian ransomware: 4 breaches (1.3%)
22. GhostR: 4 breaches (1.3%)
23. Miscellaneous countries and patriotic hacktivists: 4 breaches (1.3%)
24. North Korea (state-sponsored): 3 breaches (1%)
25. Everest ransomware: 3 breaches (1%)
26. Embargo ransomware: 3 breaches (1%)

## Key Continuities and Changes

- C10p remains the most prolific group but saw its share decrease from 26% to 17% year-over-year.
- Despite this decline, C10p's share remains more than twice that of the next most active group (17% vs. 8.2%).
- LockBit continues to hold second place despite law enforcement disruption.
- AlphV/BlackCat disbanded in early 2024, likely due to an exit scam following the Change Healthcare attack.
- RansomHub gained prominence following AlphV/BlackCat's disbanding, positioning itself as the third most active ransomware group.

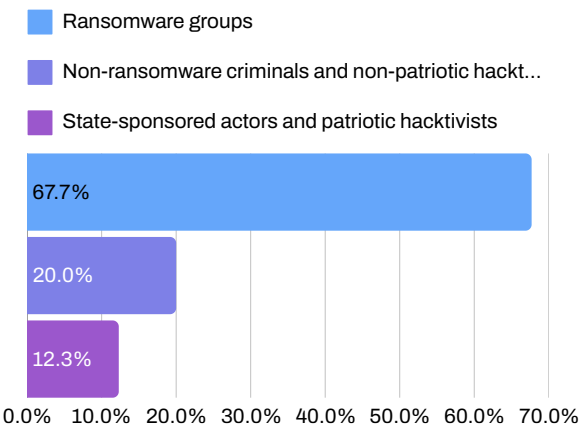
Among state-sponsored actors, China was the most prolific, with twice as many attributable breaches as Russia. This reflects a combination of factors, including China's large cyber workforce, aggressive strategy, and frequent use of third-party attack vectors.

## Third-Party Attack Specialists

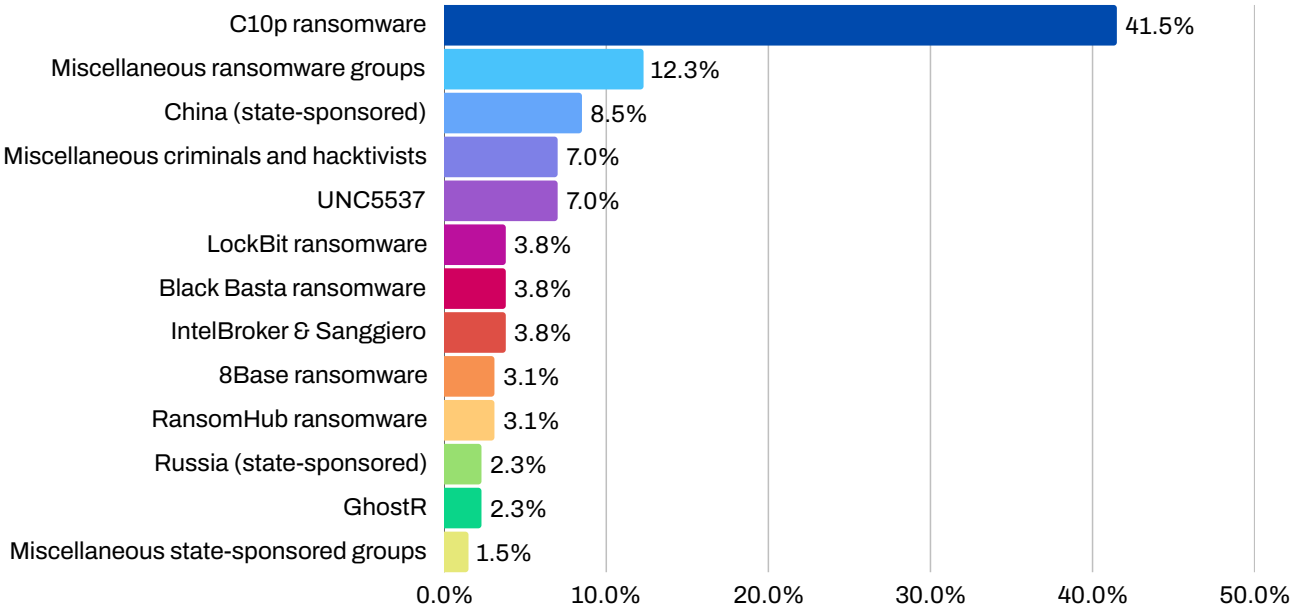
When focusing specifically on the 130 attributable breaches with third-party nexuses, the landscape shifts:

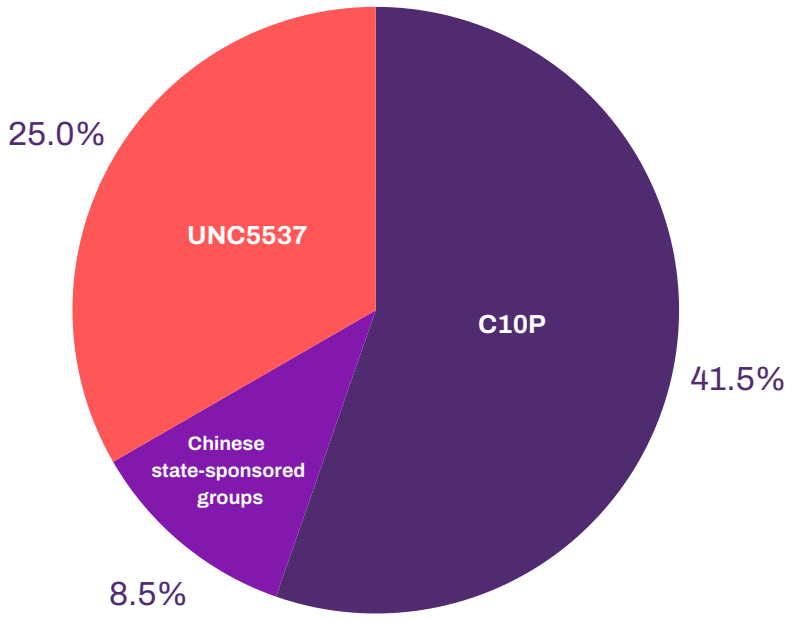
### Third-Party Breach Distribution by Threat Actor Type

- Ransomware groups: 88 breaches (67.7%)
- Non-ransomware criminals and non-patriotic hacktivists: 26 breaches (20%)
- State-sponsored actors and patriotic hacktivists: 16 breaches (12.3%)




### Top Third-Party Attack Specialists






## The Supply Chain Specialists

The data highlights that certain groups disproportionately use third-party attack vectors:

- C10p is responsible for 41.5% of attributable third-party breaches, largely due to its exploitation of zero-day vulnerabilities in file transfer software.
- Chinese state-sponsored groups account for 8.5% of attributable third-party breaches.
- Together, C10p and Chinese groups make up nearly half (49.3%) of all attributable third-party attacks.
- UNC5537 specializes in third-party attacks, such as its breaches linked to Snowflake database service compromises where accounts lacked multi-factor authentication.
- UNC5537's Snowflake campaign contributed almost one-quarter of all cloud storage compromises, making cloud storage the second most common third-party attack vector in this dataset.

These findings reinforce that third-party attack vectors offer high scalability, enabling sophisticated threat actors to compromise multiple organizations with minimal additional effort.

# Ransomware and Third-Party Attacks

## A Dangerous Symbiosis

There is a significant correlation between ransomware attacks and third-party breach vectors, suggesting that supply chain vulnerabilities are becoming increasingly central to ransomware operations.

## The Ransomware-Third Party Connection

### Key findings:

- 297 of 1,000 breaches (29.7%) involved ransomware and/or data disclosure extortion
  - Some breaches involved file-encrypting ransomware
  - Others involved extortion via the threat of data leaks
  - Some attacks involved both tactics simultaneously
- 123 of these 297 ransomware/extortion attacks (41.4%) had third-party nexuses
- These 123 incidents represent 34.6% of all third-party breaches

### Statistical correlation:

- Third-party nexuses were 5.9% more common in ransomware attacks (41.4%) than in the overall sample (35.5%)
- Ransomware attacks represented a larger share of third-party breaches (34.6%) than of overall breaches (29.7%)—a 4.9% difference
- Ransomware groups were responsible for 67.7% of attributable third-party breaches vs. 64.8% of all attributable breaches

## Why Ransomware Actors Favor Supply Chain Attacks

### Two strategic advantages explain this correlation:

### The Scalability Advantage:

- Third-party attack vectors enable attackers to compromise multiple victims through a single entry point
- This approach maximizes profits while minimizing required labor
- C10p's exploitation of file transfer software vulnerabilities exemplifies this strategy, enabling its dominant position for two consecutive years

### The Pressure Multiplier:

- Third-party data exposed in ransomware attacks creates additional leverage
- Attackers deliberately highlight compromised data from customers, vendors, and partners
- Potential damage to business relationships and reputation increases pressure on victims to pay
- This transforms third-party connections from a technical vector into a strategic pressure point

These findings likely underestimate the true correlation, as many third-party nexuses go unreported in breach disclosures. The data clearly indicates that organizations with extensive supply chains face heightened ransomware risk, requiring integrated approaches to both third-party risk management and ransomware defense.

# Third-Party Software Vulnerabilities

## When You're Only as Secure as Your Software

Our analysis reveals that third-party software vulnerabilities served as access vectors in 85 of 1,000 breaches (8.5%), with one particular campaign dominating this landscape.

## The C10p Cleo Campaign

### A Case Study in Scalable Exploitation

54 of 85 vulnerability-based breaches (63.5%) stemmed from C10p's exploitation of two Cleo file transfer software vulnerabilities:

- CVE-2024-50623
- CVE-2024-55956

This single campaign demonstrates how one actor exploiting specific vulnerabilities in widely-deployed software can create a disproportionate impact across industries.

## Beyond Cleo

### Other Critical Vulnerabilities

While most vulnerability references in our dataset were vague and lacked specific CVE identifiers, one set deserves special attention for targeting key cybersecurity organizations:

### The Ivanti VPN Vulnerabilities

Three vulnerabilities in Ivanti Connect Secure VPNs were exploited in breaches of notable security organizations:

- CVE-2023-46805 and CVE-2024-21887: Used in a breach of MITRE (the organization that manages the CVE system)
- These same vulnerabilities plus CVE-2024-21893: Used in a breach of the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA)
- Initial attribution: Chinese state-sponsored cyber espionage

## VPNs

### A Growing Attack Vector

The rise of remote work following the COVID-19 pandemic has made VPNs an increasingly popular attack vector, with two additional breaches in our sample involving VPN compromises (though specific details were unavailable).

These findings highlight the critical importance of vulnerability management, particularly for widely-deployed third-party software that can serve as a common entry point across multiple organizations.

# Customized Third-Party Risk Management Action Items

Our analysis of third-party breach patterns yields these targeted recommendations for security teams:

## Match Your TPRM Strategy to Your Risk Profile

**Third-party risk varies dramatically by:**

- Industry: Retail (52.4% third-party breach rate) vs. Education (11%)
- Geography: Northeast Asia (54.3%) vs. North America (31.9%)
- Technology: File transfer systems (14% of vectors) and cloud services (8.25%)
- Structure: Foreign subsidiaries (7.75% of vectors) vs. domestic (4%)

**Example:** A Japanese technology company with a Taiwanese subsidiary competing against Chinese firms faces significantly higher third-party risk than a U.S. hospital. The technology company's profile combines Japan's 60% third-party breach rate, technology sector vulnerability (47.3%), and potential Chinese state targeting of its Taiwanese operations (57.1% third-party breach rate).

## Mitigate Fourth-Party Risk

**The 45 fourth-party breaches we documented show how risk cascades through supply chains:**

- Require vendors to maintain their own robust TPRM programs
- Include TPRM requirements in vendor contracts
- Recognize that inadequate vendor TPRM exposes your organization to fourth-party risk

## Demand "Secure by Design" Technology

**Technology products enabled 46.75% of third-party breaches:**

- Require security features to be default and central, not optional
- Integrate security requirements into procurement standards
- Support CISA's "Secure by Design" initiative through vendor selection

## Harden High-Risk Infrastructure

**Prioritize defense of:**

- File transfer software (14% of third-party breach relationships)
- Cloud infrastructure (8.25%)
- Industry-specific services (healthcare: 15.75%, financial services: 11.75%)
- VPN systems (increasingly targeted post-pandemic)

Take immediate action through prompt patching, multi-factor authentication, and regular assessments.

## Avoid Ransomware Payments

**With ransomware involved in 41.4% of third-party breaches:**

- Payments create legal risk (potential sanctions violations)
- Funding enables future attacks
- Decryption often fails or is incomplete
- Attackers frequently demand additional payments
- Data is frequently leaked despite payment

Your ransom avoidance protects both your organization and the broader security community.

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

## ABOUT SECURITYSCORECARD

SecurityScorecard created Supply Chain Detection and Response (SCDR), transforming how organizations defend against the fastest-growing threat vector—supply chain attacks. Our industry-leading security ratings serve as the foundation and core strength, while SCDR continuously monitors third-party risks using our factor-based ratings, automated assessments and proprietary threat intelligence, to resolve threats before they become breaches. MAX enables response and remediation capability, working through our service partners to protect the entire supply chain ecosystem while strengthening operational resilience, enhancing third-party risk management, and mitigating concentrated risk.

Trusted by over 3,000 organizations—including two-thirds of the Fortune 100—and recognized as a trusted resource by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Backed by Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, NGP, Intel Capital and Riverwood Capital, SecurityScorecard delivers end-to-end supply chain cybersecurity that safeguards business continuity. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

**SecurityScorecard.com**
info@securityscorecard.io