

REPORT

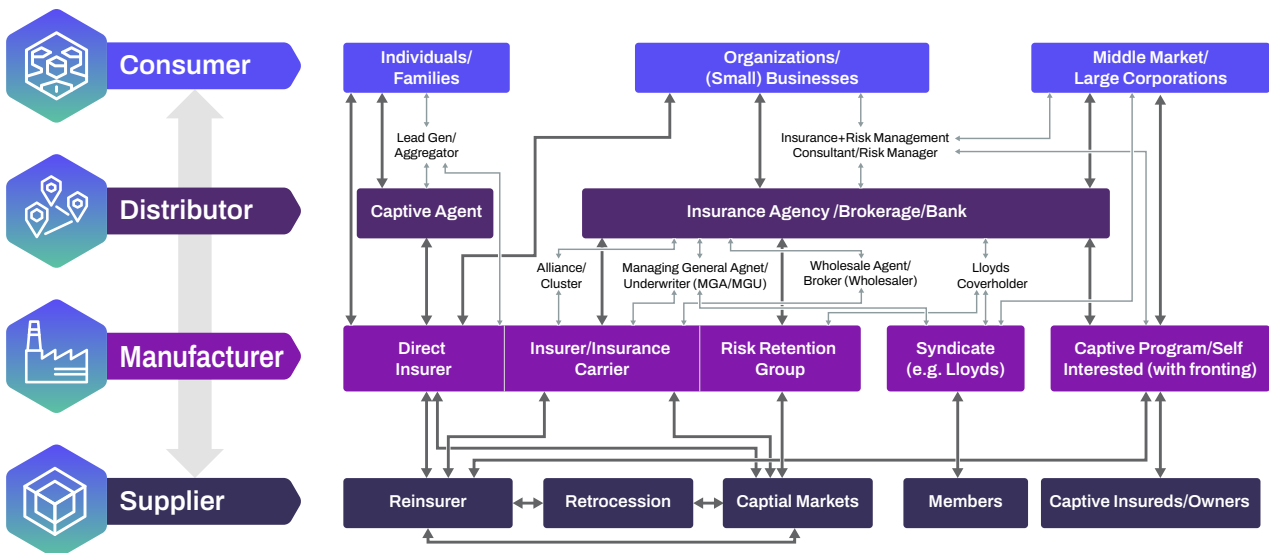
# A Cyber Security Assessment of the Insurance Industry Supply Chain

# Introduction

The insurance industry’s supply chain plays a vital role in providing services to millions, but it also creates opportunities for cyber risks. This report explores the cybersecurity challenges in this industry, focusing on weaknesses in its supply chain that contribute to third-party risks. By reviewing the SecurityScorecard ratings and breach histories of 150 top companies worldwide, we offer clear insights into the state of cybersecurity across the sector.

## Our research organizes the supply chain into five main segments:

1. Insurance carriers: Core entities that provide policies to consumers and businesses.
2. Reinsurance: Companies that insure insurance carriers, sharing financial risks.
3. Agencies and brokers: Businesses responsible for selling and distributing insurance products.
4. Third-party claims processors and administrators: Organizations managing claims on behalf of insurers.
5. Insurance-specific software and IT products and services: Technology providers offering specialized tools and systems for the industry.



This structure helps pinpoint where risks originate and how they affect the industry as a whole. The list of 150 companies was carefully assembled using reliable insurance industry [publications and rankings](#), ensuring accuracy and depth in our findings.

# Summary

## Overall Security Posture

Our analysis of the insurance industry's security posture offers a mixed picture. Average security scores match those of other industries, yet 23% of companies have unsatisfactory ratings, which raises concerns.

## Implications for Insurance Carriers

Insurance carriers should focus on these underperformers. Their partners across all four other insurance segments score even lower, increasing third-party risk. This heightened exposure likely explains why insurance carriers are overrepresented among breached insurance companies—both in general and for third-party breaches in particular.

## Third-Party Breaches and Supply Chain Exploits

Higher average scores did not shield companies with third-party breaches from attack. In fact, threat actors may have intentionally targeted better-defended firms through weaker links in their supply chains. The data confirms this: the third-party breach rate in this sample (59%) is the highest SecurityScorecard has documented so far, and more than twice the global cross-industry average. Notably, the leading cause (37%) of actual third-party breaches—general cross-industry software and IT products and services—originated outside the insurance sector.

## Dominance of Ransomware Attacks

Ransomware remains the top threat to this industry, as it is with many others. Still, the degree to which ransomware dominated this sample, overshadowing other threats, surprised our researchers. A strong correlation exists between ransomware and third-party breaches, and their overlap is significant. Third-party attack vectors let ransomware operators scale their operations efficiently, infecting many targets at once.

## Geographic Variations in Risk

Geographic differences highlighted two countries. Chinese companies were the only ones with markedly below-average scores, introducing yet another source of cyber risk for their foreign partners beyond well-known concerns about their government. Despite these lower Chinese scores, U.S. companies experienced higher metrics of actual compromises, including publicly reported breaches and compromised credentials. The U.S. in general is a top target for threat actors worldwide due to the size and global dominance of its economy, the geopolitical power of its government, and its use of English.

# Key Findings

## Overall Security Posture

- Average insurance security scores (86/88) align with most other industries, yet only 77% of companies earned A or B grades, compared to at least 81% in other sectors. Only the S&P 500 and U.S. healthcare & pharmaceuticals had higher average scores.
- The top three cyber risk factors are Application Security (40%), DNS Health (29%), and Network Security (20%). DNS Health rarely ranks this high.
- The top three security issues all involve weak or missing encryption: weak SSL/TLS protocols, unencrypted redirect chains, and unencrypted cookies.
- Malware infections and device compromises affected 17% of companies last year, though the overall severity was less than that percentage suggests.
- More than half (56%) had at least one compromised credential in the past two years. U.S. insurance carriers had the most compromised credentials by wide margins, skewing the data (median: 15; mean: 433).
- 28% of companies reported breaches—higher than the S&P 500 (21%) and double the U.S. energy industry (14%), though not as high as U.S. federal contractors (35%).

## Implications for Insurance Carriers

- Insurance carriers and reinsurance providers have the highest average scores, while agencies & brokers and insurance-specific software & IT vendors score the lowest. This score gap increases carriers' third-party risk.
- Breach rates were highest for the U.S. insurance industry overall, including both carriers and agencies & brokers.
- Of the 42 breached companies, 12 experienced multiple breaches. These multi-breach firms were mostly U.S.-based carriers or agencies & brokers.

## Third-Party Breaches and Supply Chain Exploits

- Third-party breaches reached 59%, the highest rate observed so far and more than double the global cross-industry average of 29%.
- Companies with third-party breaches often had above-average scores (mean/median: 88/89), suggesting attackers circumvented strong defenses by exploiting weaker partners.
- Third-party software & IT caused 50% of these breaches. Cross-industry software & IT accounted for 37%, far outpacing insurance-specific IT (13%).
- The 2023 MOVEit file transfer software campaign led to many of these breaches, either directly or as fourth-party incidents.

## Dominance of Ransomware Attacks

- Ransomware is the top threat to the insurance industry, exceeding its dominance in most other sectors.
- Every attack tied to a known threat actor involved ransomware.
- Ransomware and third-party breaches strongly overlap, allowing attackers to infect multiple targets at once via supply chain vulnerabilities.

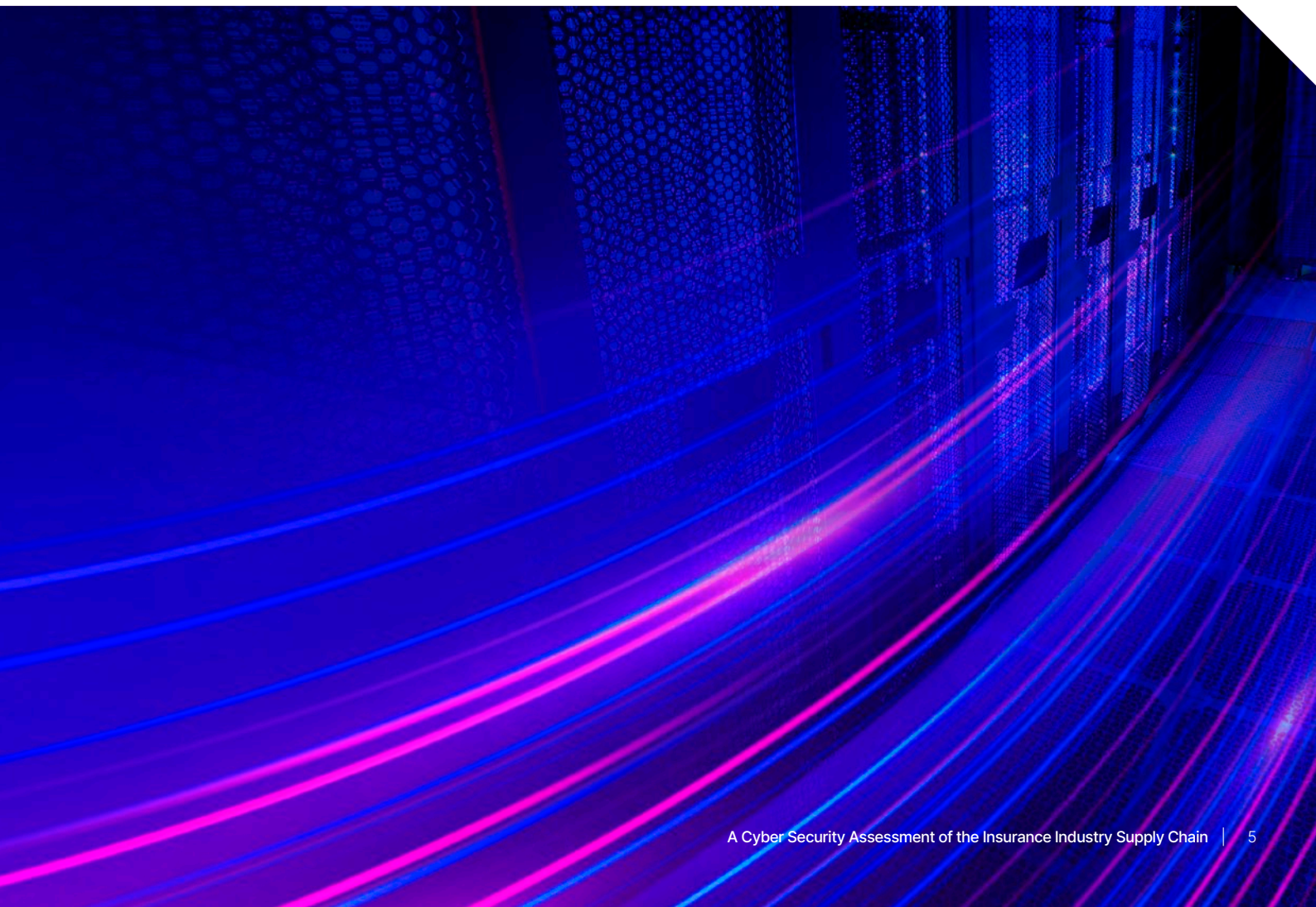
## Geographic Variations in Risk

- Only Chinese insurance companies have notably lower scores (79/79), adding to third-party risk beyond known geopolitical factors.
- The highest breach rates were found in the U.S. insurance industry overall and specifically among U.S. carriers and agencies & brokers.

# Methodology

We based our analysis on non-intrusive scans of each company's publicly visible attack surface and records of known breaches. For each company in our sample, we collected:

- **Industry Segment & Location:** The company's primary industry segment and its main geographic base.
- **Overall Security Score:** A comprehensive rating informed by SecurityScorecard's scans and evaluations of the company's publicly accessible infrastructure and historical breaches.
- **Lowest-Scoring Risk Factor:** The security category where the company earned its weakest sub-score.
- **Key Negative Issue:** The specific issue that most significantly lowered the company's overall score.
- **Evidence of Compromise:** Any signs of malware infections or device compromises within the past year, as well as compromised credentials identified within the past two years.
- **Breach History:** Details of any publicly reported breaches, including whether they originated from third-party vendors or partners, and any identified threat actors behind them.

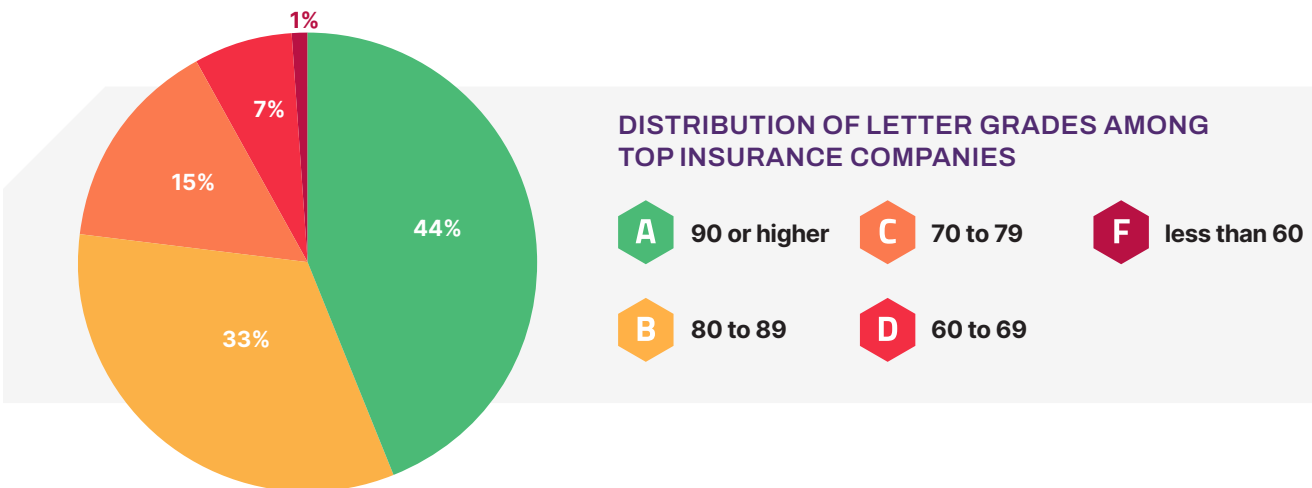


# General Statistics

## Overall Security Scores

The mean overall security score for our insurance industry sample is 86 out of 100, and the median is 88. This indicates a slightly “left-skewed” distribution, where a few very low scores pull the mean down below the median.

A mean score of 86 compares favorably with our global mean of 83 across more than 12 million organizations. It also aligns with other industry samples we analyzed, including the U.S. energy industry (86/88), top 150 U.S. federal government contractors (86/88), the global aviation industry (85/88), and the top 150 technology vendors (84/87). However, it falls short of the U.S. healthcare & pharmaceuticals industry and the S&P 500, both of which average 88/89.



### According to our rating methodology:

- A “B” rating indicates a 2.9x greater likelihood of a breach than an “A.”
- A “C” indicates a 5.4x greater likelihood than an “A.”
- A “D” indicates a 9.2x greater likelihood than an “A.”
- An “F” indicates a 13.8x greater likelihood than an “A.”

In broad terms, “**A**” is strong or excellent; “**B**” is good or respectable; and “**C**,” “**D**,” and “**F**” are weak, deficient, or bad.

## Comparison with Other Industries

In this insurance sample, 77% of companies have strong (A) or good (B) ratings, while 23% fall into weak, deficient, or bad categories (C, D, or F). This 77% strong/good proportion matches that of [global aviation](#) (77%) and [top 150 technology vendors](#) (77%). It is, however, four points lower than the [U.S. energy industry](#) (81%) and well below the [S&P 500](#) (88%) and [U.S. healthcare & pharmaceuticals](#) (90%).

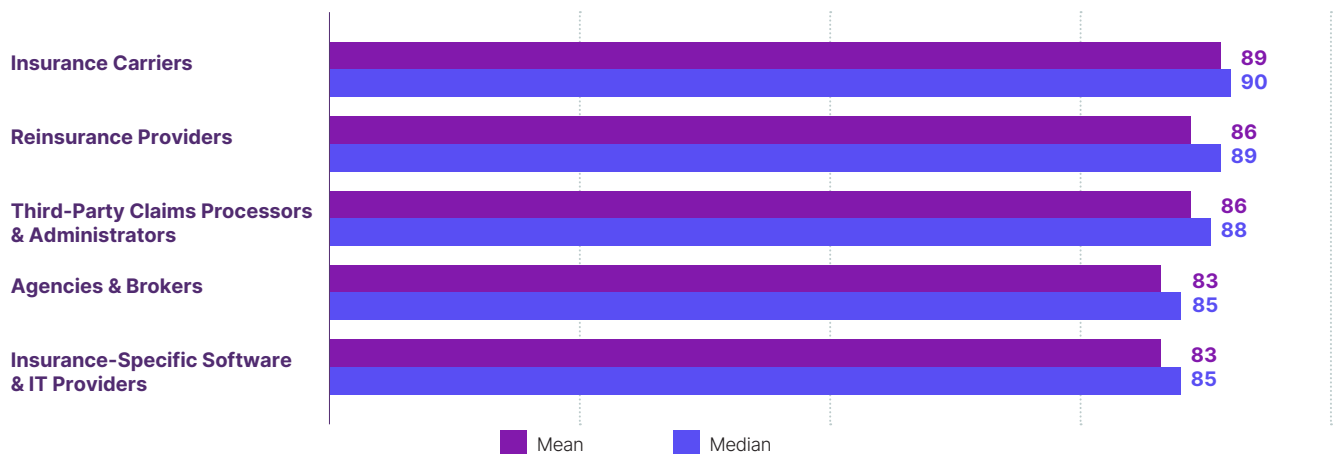
## Implications

These results suggest that most insurance companies maintain strong or good security postures, but a significant minority lags behind. Since a security posture is only as strong as its weakest link, companies with weak ratings pose heightened third-party cyber risk for their partners and customers in other industry segments. The following sections will examine where these security weaknesses are most pronounced.

# Variations by Industry Segment

We divided the industry into five supply chain segments and measured their mean and median scores:

MEAN/MEDIAN SECURITY SCORES BY INSURANCE INDUSTRY SEGMENT



Although all of these scores fall within a relatively close range (in the 80s), the differences are meaningful enough to group them into three tiers:

- High (Insurance Carriers and Reinsurers)
- Medium (Third-Party Claims Processors & Administrators)
- Low (Agencies & Brokers and Insurance-Specific Software & IT)

This stratification matters. Carriers and reinsurers, whose core business involves paying claims, face stringent regulatory scrutiny and solvency requirements. This likely fosters a stronger risk management culture and translates into more mature security practices. As a result, carriers and reinsurers achieve higher scores, placing them at the top tier of the industry.

Third-party claims processors sit in the middle. Although they manage sensitive claim data, they may not face quite as much regulatory pressure as carriers or reinsurers, which can lead to slightly lower scores.

At the lower end, agencies & brokers and insurance-specific software & IT providers stand out. Their lower scores align with a pattern observed in other industries: providers of IT products and services often rank lower than their customers. While factors such as cloud or SaaS

environments can occasionally complicate asset attribution and scoring, those complexities alone do not fully explain the lower scores. Instead, these vendors may have genuine security challenges—misconfigurations, vulnerabilities, or larger and more complex attack surfaces—that weaken their security posture.

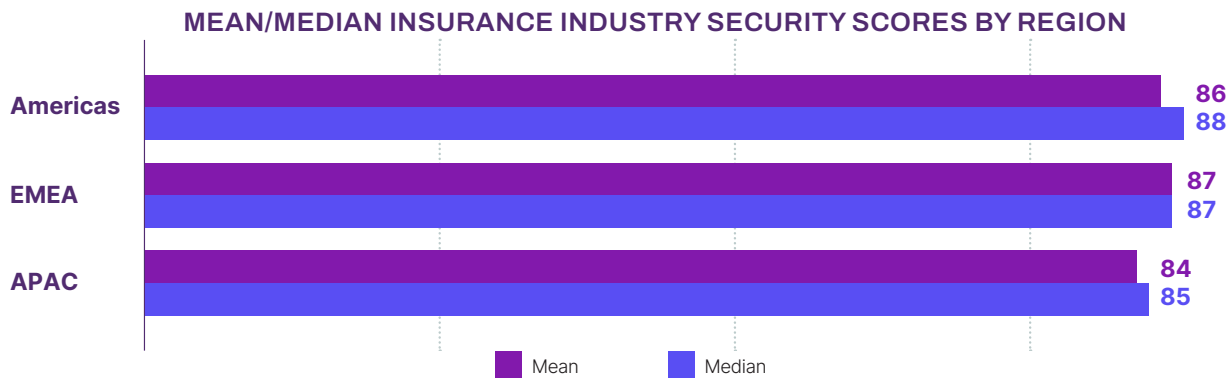
Agencies & brokers, meanwhile, typically maintain a strong customer-facing presence. This can increase exposure to social engineering attacks and other security threats. Although our current scoring for social engineering risk is limited, the high visibility and accessibility inherent in sales operations generally create more “attack surface.” Threat actors can easily identify potential targets in these roles, and the push for sales and responsiveness may reduce the caution that staff exercise when interacting with unknown parties. Public-facing infrastructure also heightens the risk of vulnerabilities or misconfigurations that attackers can exploit.

These distinctions mirror patterns we have seen elsewhere. In our analysis of the global aviation industry, airlines scored higher than every supporting segment, just as insurance carriers outscore the vendors and brokers that support them. In both industries, the central organizations that bear the greatest financial and regulatory burdens demonstrate stronger overall security postures. In turn, they rely on lower-scoring partners or vendors, which amplifies third-party risk within their respective ecosystems.

# Variations by Geography

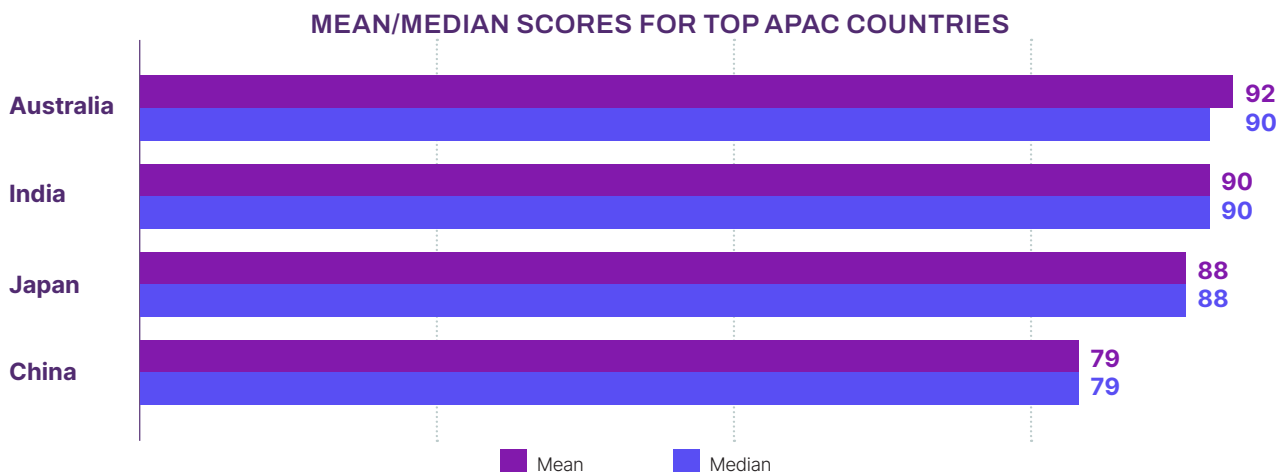
We examined scores across three major regions: the Americas, EMEA, and APAC.

## Regional Overview



Overall, the Americas (primarily U.S. firms) and EMEA (mostly Western European companies) scored higher than the APAC region. This trend aligns with [our previous research showing](#) a correlation between security ratings and economic factors like GDP per capita. Regions with more developed economies tend to have stronger security postures.

## The China Effect in APAC



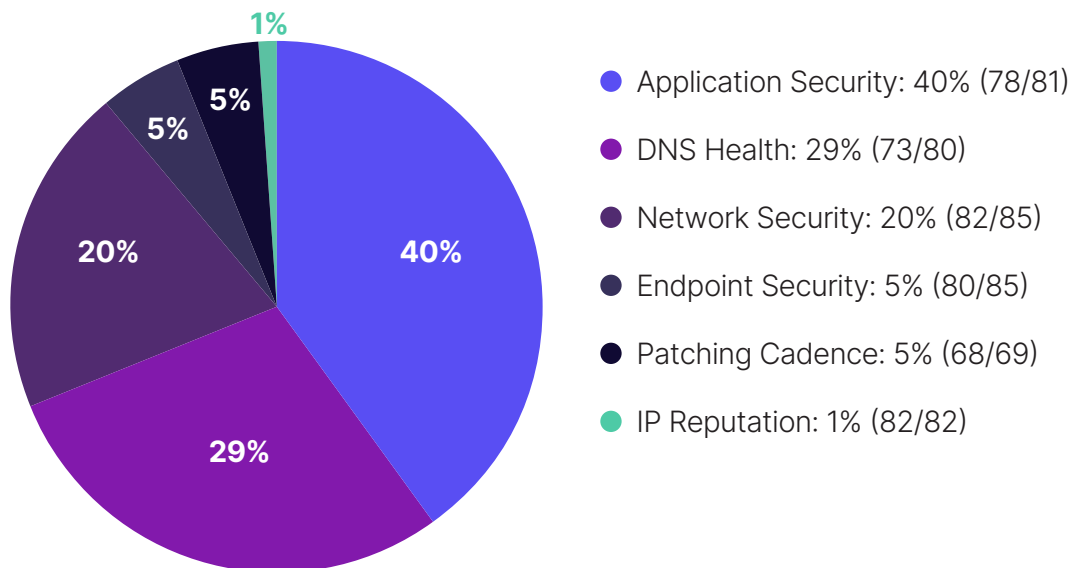
Chinese businesses already pose inherent third-party cyber risk due to Chinese government-sponsored cyber espionage. Now these lower security scores add another layer of concern for foreign partners. The weaker security postures of Chinese insurance firms could unwittingly expose their overseas counterparts to third-party breaches and network compromises.

# Common Security Risks

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.

## Security Overview

PERCENTAGES OF COMPANIES SCORING LOWEST IN EACH SECURITY FACTOR, WITH THEIR MEAN/MEDIAN SCORE



### Observations:

- Application Security is the most common lowest-scoring factor by a wide margin. This matches patterns observed in other industries.
- DNS Health, while often present, rarely ranks as high as it does here, where it comes in second.
- Network Security typically appears among top risks but usually scores lower than Application Security. In this sample, it ranks third instead of first or second.
- Endpoint Security scores, often a common issue, are less prominent here at only 5%.
- Patching Cadence affects a small number of companies (5%), but for those affected, it has the lowest mean/median sub-scores (68/69), making it uniquely impactful despite its low frequency.
- IP Reputation rarely emerges as a lowest-scoring factor (1%).

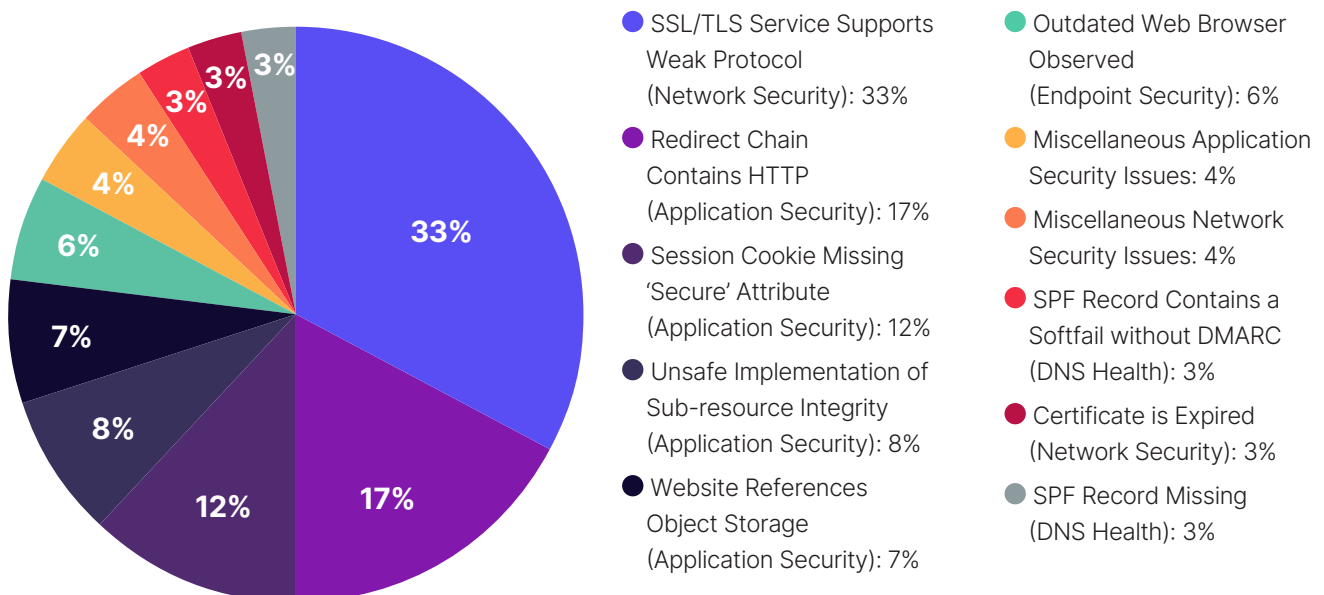
### Specific Security Issues

We further examined the individual issues within each factor that had the most negative impact on scores. The list below shows these issues and their frequency in the sample, along with their associated security factor. We consolidated several less common Application Security and Network Security issues into “Miscellaneous” categories.

# Specific Security Issues

We further examined the individual issues within each factor that had the most negative impact on scores. The list below shows these issues and their frequency in the sample, along with their associated security factor. We consolidated several less common Application Security and Network Security issues into “Miscellaneous” categories.

## SECURITY ISSUES WITH MOST NEGATIVE SCORE IMPACT FOR EACH COMPANY



### Key Insights:

- Application Security issues account for almost half (48%) of the highest-impact problems, in line with Application Security's prominence as a lowest-scoring factor.
- Network Security issues represent 40% of the most impactful problems, mainly due to one critical issue—weak SSL/TLS protocols—affecting one-third (33%) of companies.
- Weak SSL/TLS is a recurring major concern, indicating widespread use of outdated encryption methods or configurations.

## Focus on Encryption and Unencrypted Traffic

Two of the top Application Security issues involve unencrypted traffic:

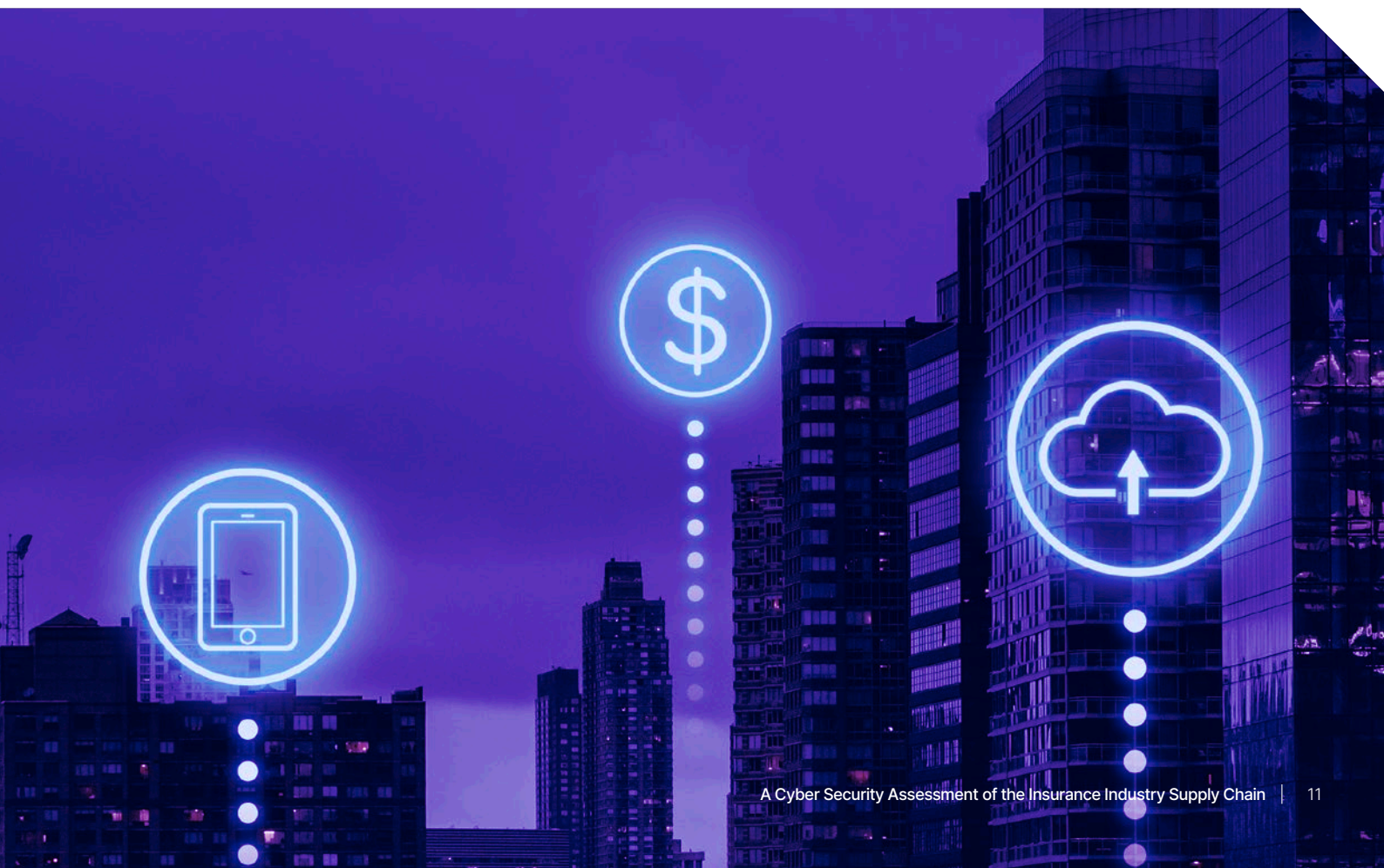
- Redirect Chain Contains HTTP (17%): Unencrypted redirects expose users to interception and redirection to malicious infrastructure.
- Session Cookie Missing 'Secure' Attribute (12%): Without the "secure" attribute, cookies travel unencrypted over HTTP, risking theft by attackers.

These vulnerabilities facilitate man-in-the-middle (MITM) attacks and phishing attempts, significantly raising the risk profile.

## DNS Health Issues

Despite DNS Health often ranking high as a lowest-scoring factor, only two DNS Health issues made this top-impact list, each at 3%. Both relate to Sender Policy Framework (SPF) records, which help prevent email spoofing. Missing or misconfigured SPF records increase the likelihood of phishing and fraud campaigns.

In summary, Application Security and Network Security stand out as key areas of concern, with encryption-related vulnerabilities posing particular risks. While DNS Health ranks high as a factor, it contributes fewer top-impact issues than Application Security or Network Security. The results highlight the need for stronger encryption practices, proper configuration of DNS records, and vigilant patching to improve overall security postures.



# Malware Infections and Compromised Devices

## Signs of Compromise and IP Reputation

Our IP Reputation security factor tracks potential malware infections or other signs of device compromise within the past year. We detect these compromises through intelligence sources like sinkholes and honeypots. Such findings can involve various threats, including ransomware, information stealers, adware, and other types of malware, as well as the malicious repurposing of compromised devices for attacks, scans, or use by the TOR network.

## Context and Limitations

It is important to note that these indicators do not necessarily confirm a full-scale breach. An alert may represent just one infected or compromised device. However, such activity could hint at undetected breaches or early-stage intrusions. A single compromised device might serve as a foothold for lateral movement and deeper network penetration by threat actors.

## Comparisons Across Industries

Out of 150 companies, 25 (approximately 17%) showed signs of at least one infection or compromised device in the past year. This rate matches the global aviation industry's figure (17%), is more than double that of the U.S. energy industry (8%), and falls well below that of the top 150 technology vendors (41%).

## Narrow Range of Threat Types

Closer examination reveals a more favorable picture of the insurance industry. Unlike other samples, where multiple categories of malware and repurposed devices appear, only two categories—Adware and “Malware” (a category excluding adware, ransomware, and information stealers)—were present in this sample. Crucially, several categories were completely absent, including information stealers, ransomware, and all forms of malicious device repurposing. The absence of these more severe threats is unusual and suggests a comparatively limited scope of infections.

## Severity and Scale of Infections

Among the 25 affected companies, 22 had only adware infections. Adware is generally considered a less severe threat compared to information stealers, ransomware, or other advanced malware. Most companies recorded only a few infections (single-digit counts). Only one company had 10 or more infections on its network—still relatively low compared to other industries, where numbers can reach triple digits.

In summary, while 17% of companies displayed signs of compromise, these infections were typically low-severity and low-volume. This distinction sets the insurance industry sample apart from others, showing that while compromise indicators exist, they are relatively contained and less serious than those observed elsewhere.

# Compromised Credentials

We expanded our analysis to another indicator of compromise: credentials harvested by information stealers. Our platform tracks compromised credentials for each organization over the past four months and two years. When both timeframes were available, we averaged the two figures; otherwise, we used the single timeframe available.

## Overall Frequency and Distribution

Out of 150 companies, 84 (56%) had at least one compromised credential in the past two years. The number of compromised credentials per company ranged widely, from 1 to 3,350. The median was 15 and the mean was 433, indicating a “right-skewed” distribution. In other words, a small number of companies with very high counts heavily influenced the mean, making the median a more accurate reflection of the overall data set..

## Concentration Among U.S. Insurance Carriers

To understand the minority of companies with significantly higher numbers of compromised credentials, we focused on the 28 companies at the upper end of the scale. Each of these 28 companies had 200 or more compromised credentials, placing them in the top one-third of the 84 companies with such incidents.

- 22 of the 28 (**79%**) were insurance carriers, despite carriers representing only about **27%** of the overall sample.
- 22 of the 28 (**79%**) were also U.S.-based, even though U.S. companies accounted for only **56%** of the total sample.

This makes U.S.-based insurance carriers disproportionately represented among those with the largest numbers of compromised credentials. Many of these U.S. carriers are major, recognizable brands known to consumers through their policies or advertising. Their prominence may make them more attractive targets, leading to greater numbers of compromised credentials.

# Publicly Reported Breaches

SecurityScorecard's intelligence sources—ranging from mainstream media to regulatory disclosures and underground forums—document publicly reported breaches for correlation with security signals. Breaches can influence an organization's score, especially when data disclosures (such as compromised credentials or network details) give attackers actionable information for future attacks.

## Frequency of Breaches

Out of **150** companies, 42 (**28%**) experienced at least one publicly reported breach, resulting in a total of **64** breaches. While not the highest breach rate observed in previous research (e.g., **35%** for top 100 U.S. federal contractors), it is twice the rate of the top 250 U.S. energy companies (**14%**).

## Multiple Breaches

These 42 breached companies accounted for 64 total breaches, indicating that some companies experienced multiple incidents:

- 30 companies had 1 breach each (30 total breaches)
- 6 companies had 2 breaches each (12 total breaches)
- 4 companies had 3 breaches each (12 total breaches)
- 1 company had 4 breaches (4 total breaches)
- 0 companies had 5 breaches
- 1 company had 6 breaches (6 total breaches)

## Demographics of Breached Companies

Breached companies disproportionately came from specific regions and segments:

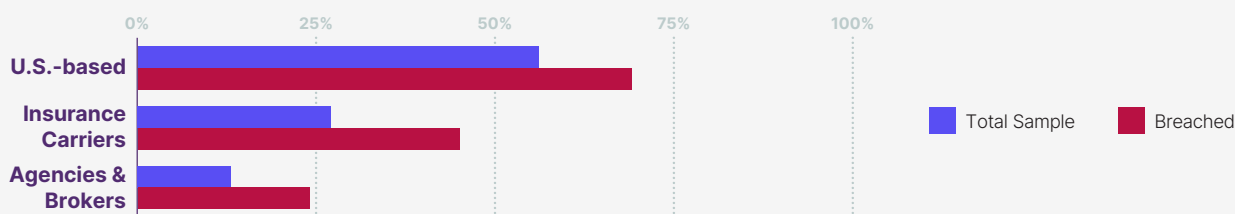
- **U.S.-based:** 56% of the entire sample was U.S.-based, but these companies made up 69% of breached organizations.
- **Insurance Carriers:** Approximately 27% of the total sample were carriers, but 45% of the breached companies fell into this segment. About half of all carriers in our sample experienced a breach.
- **Agencies & Brokers:** About 13% of the sample were agencies & brokers, yet they represented 24% of the breached organizations. Roughly half of all agencies & brokers were breached.

Among the **12** companies with multiple breaches, these patterns intensified:

- **9 of the 12** companies with two or more breaches (75%) were U.S.-based.
- **8 of these 12** companies (approximately 66%) were insurance carriers.

The data highlights that U.S.-based companies, particularly insurance carriers and agencies & brokers, face disproportionately high breach rates. The frequency of breaches—and especially multiple breaches—is most pronounced among U.S.-based insurance carriers and, to some extent, U.S.-based agencies & brokers.

### DISTRIBUTION OF BREACHES PER COMPANY



# Third-Party and Fourth-Party Breaches

## Extent of Third-Party Breaches

Out of the 64 total breaches, 38 (approximately 59%) involved third parties. These breaches either compromised another organization's infrastructure or data, or reached the target via a vendor or another third party. This 59% third-party breach rate is higher than any other industry-specific sample we have analyzed, surpassing the previous record of 58% among top U.S. federal contractors. It also far exceeds the [global cross-industry baseline of 29%](#).

## Surprising Findings Among High-Scoring Companies

Thirty companies (20% of our total sample) experienced at least one third-party breach. Surprisingly, these companies had slightly higher mean/median security scores (88/89) than the overall sample. Since these scores reflect only the organizations' own security postures—and not those of their vendors—this suggests that threat actors deliberately targeted strong organizations through weaker third-party links. An otherwise robust security program can still falter if partners in its supply chain have weaker security postures, creating opportunities for attackers.

## Impact on Insurance Carriers

Insurance carriers were disproportionately affected by third-party breaches. Although carriers made up about 27% of the total sample, they represented 50% of the 30 companies hit by third-party incidents. This outcome aligns with carriers' position at the "receiving end" of the supply chain. They rely on the other four, generally lower-scoring segments of the industry, which heightens their third-party risk.

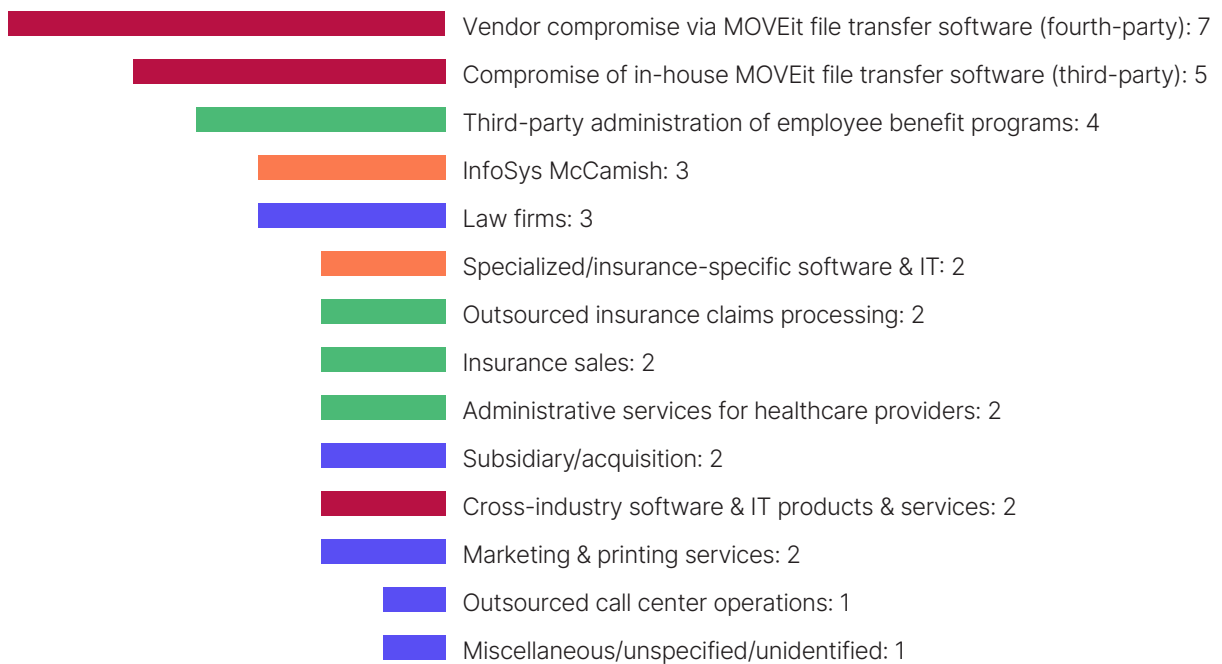
## Fourth-Party Breaches

A portion of these third-party breaches were actually "fourth-party" incidents, where the initial compromise originated even further down the supply chain. Ten breaches in our sample, about 16% of the total and 26% of the third-party subset, fit this description. This fourth-party risk underscores the importance of thoroughly evaluating not only direct vendors but also their own suppliers and partners.

# Products & Services That Enable Third-Party and Fourth-Party Breaches

Identification of the various types of relationships that enable third-party breaches can help TPRM teams prioritize different types and sources of risk for varying levels of scrutiny. Below is a pie chart of the relationships described in the reporting on the subset of third-party breaches, based on the nature of the product or service that enabled the breach.

## PRODUCTS AND SERVICES ENABLING THIRD-PARTY BREACHES



### We grouped these items into four categories.

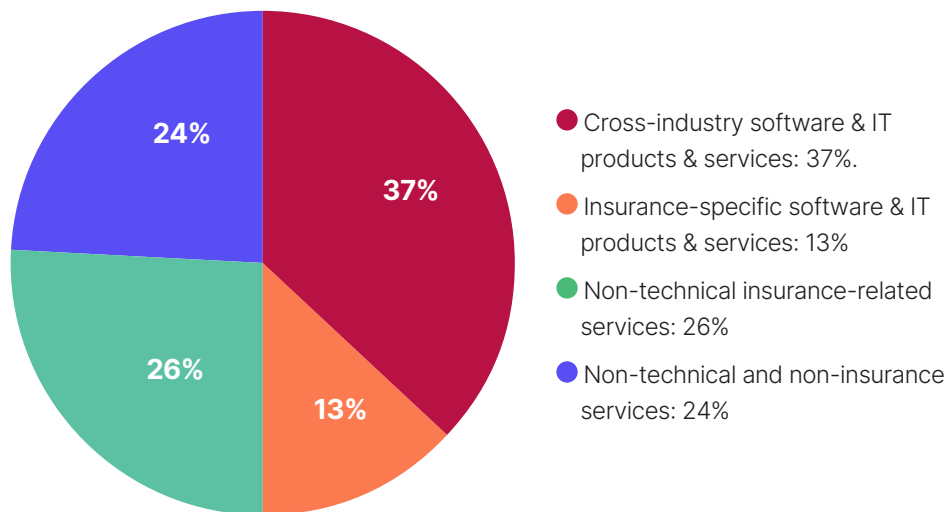
Shaded in red are cross-industry software & IT products & services. The three items in this category accounted for 14 of the 38 third-party breaches, or approximately 37%.

Shaded in orange are insurance-specific software & IT products & services. These two items accounted for 5 of the 38 third-party breaches, or approximately 13%.

Shaded in green are non-technical insurance-related services. The four items in this category accounted for 10 of the 38 third-party breaches, or approximately 26%.

Shaded in blue are providers of various non-technical and non-insurance products and services or other miscellaneous relationships. The five items in this category accounted for 9 of the 38 third-party breaches, or approximately 24% of them.

## CATEGORIES OF RELATIONSHIPS ENABLING THIRD-PARTY AND FOURTH-PARTY BREACHES



These four categories form two halves, both of which account for 50% each of the subset of third-party breaches. The red & orange half represents software & IT products & services, including both cross-industry and industry-specific offerings. The green & blue half represents non-technical services, including both those within and those outside the insurance industry.

We previously identified software & IT products & services as top sources of third-party risk in general - responsible for as much as 75% of third-party breaches, according to our last global report. The figure of 50% for our insurance industry sample is significantly lower but still high.

Of greater interest is the imbalance between cross-industry and industry-specific products and services (37% vs. 13%). In certain industries, such as financial services and healthcare, industry-specific software & IT are top enablers of third-party breaches. Given the relationships of insurance with those two industries, one might expect a similar pattern to hold true for insurance, but it does not. The salience of cross-industry software in this sample of third-party breaches is due largely to the massive 2023 campaign to exploit a zero-day vulnerability (CVE-2023-34362) in MOVEit file transfer software across all industries.

The MOVEit campaign affected companies directly, via their own in-house installations of the software, and indirectly in fourth-party breaches of vendors with their own MOVEit installations. It is worth noting that fourth-party MOVEit data breaches outnumbered compromises of in-house MOVEit installations in our sample (7 to 5). One insurance company had [two separate fourth-party MOVEit breaches](#) via [two separate vendors](#). Another company was involved in two separate fourth-party MOVEit breaches. One of them exposed data on the company's retail customers via [a MOVEit breach at one of its vendors](#). That same company also exposed data from one of its own customers via [a compromise of its own in-house MOVEit installations](#).

The share of third-party breaches attributable to industry-specific software & IT includes [three insurance third-party victims](#) of a [LockBit ransomware](#) attack on [InfoSys McCamish](#). We treated these examples as insurance-specific insofar as that IT services vendor specializes in supporting financial services and insurance companies, who dominated the list of its third-party victims.

# Illustrative Examples of Third-Party and Fourth-Party Breaches

The practice of outsourcing of various insurance tasks and services to other insurance companies deserves special consideration, highlighting the risk of trusting one's vendors and other partners within the industry. Indeed, three segments of the industry exist just for this purpose: third-party claims processors & administrators; agencies & brokers; and insurance-specific software & IT.

Outsourcing claims processing to other companies poses the risk of exposing customer claims data (if not other data or infrastructure) in the event of a breach at that claims processor. For example, a RagnarLocker ransomware attack on third-party claims processor Gallagher Bassett exposed information on policyholders of its carrier customers, including [QBE North America](#).

Third-party administrators of employee benefit programs, which often include health and/or life insurance, are another source of third-party risk. For example, [a breach at Keenan & Associates](#), the third-party administrator of Prime Healthcare's health benefit plan for its own employees, experienced a breach that exposed information on those beneficiaries.

Some health insurance carriers arrange outsourced administrative services for healthcare providers that contract with them. A breach at those companies poses third-party risk for those insurance carriers. For example, [a breach at Prospect Medical](#), which provides administrative services to healthcare providers contracting with health insurance carrier Humana, as well as [Prudential's health plans](#), exposed patient data that it had received from both carriers.

Breaches at agencies & brokers that sell insurance for carriers can also expose insurance customer data. For example, a breach at Choice Health, an independent insurance broker, compromised policyholder data for Humana. [Choice Health sold Medicare products for Humana](#).

Another source of third-party risk is obtaining a specific type of coverage for one's policyholders from another insurance carrier that is not available among one's own plan offerings, or working with another carrier to manage such coverage. [In an example of fourth-party breach](#), policyholders of Nippon

Life Insurance Company of America, which arranged vision coverage for its customers via EyeMed, had their personal and insurance information exposed via a breach at a fourth-party: the law firm Orrick, Herrington & Sutcliffe, which represented EyeMed.

Insurance-specific software is another source of third-party risk within the industry. [In a glaring example](#), a security misconfiguration in the QQCatalyst insurance agency management platform that exposed customer data went undetected for more than eight years, despite the acquisition of its company QCSolutions by Vertafore. The misconfiguration had been present since the release of this software in 2012 and remained undetected despite any due diligence during the 2015 acquisition. The misconfiguration only came to light in 2020, after a separate, unrelated data-exposing misconfiguration at Vertafore prompted a review of its security posture. The misconfiguration affected at least 42,000 customers of at least 16 insurance agencies, if not more.

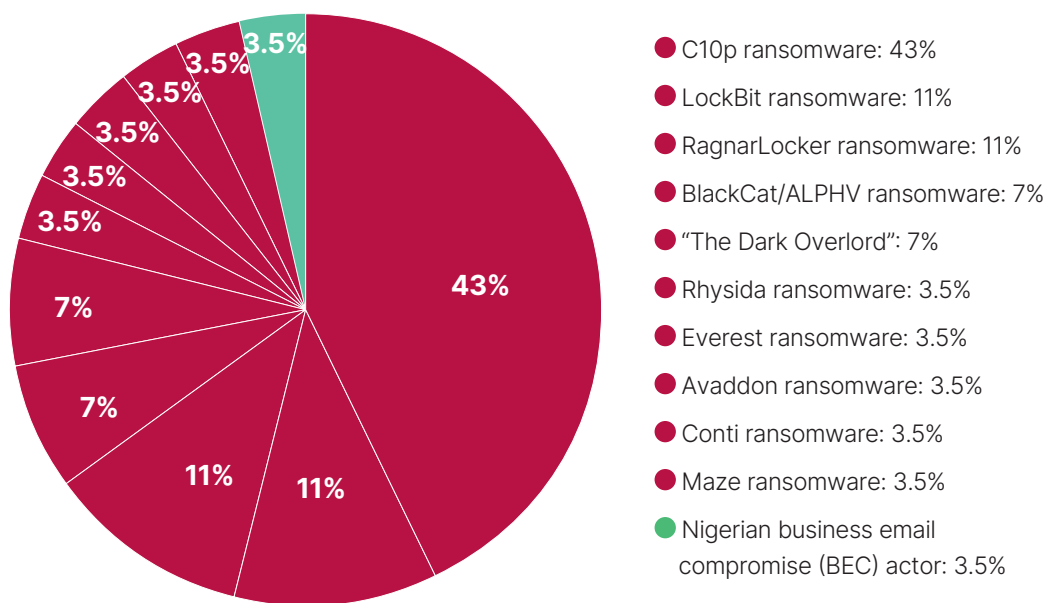
As for non-technical sources of cyber risk from outside the industry, law firms deserve special consideration, both in general and for insurance companies in particular. They frequently surface as unwitting non-technical enablers of third-party breaches when they experience data breaches that expose their corporate clients' data. Law firms are of particular interest to insurance companies insofar as the latter often engage in more litigation than companies in other industries.

In a classic example of such a third-party breach, the threat actor "The Dark Overlord" claimed to have obtained data on litigation surrounding the 9/11 terrorist attacks from insurance companies such as Hiscox Syndicates and Lloyd's of London. Hiscox later clarified that [the compromised data came from a breach of a law firm representing it in 9/11-related litigation](#).

# Threat Actor Attribution

28 of the breaches in our sample were attributed to specific threat actors, according to the reports. Below is a pie chart illustrating the distribution of attacks attributable to various actors. Criminal ransomware groups are shaded in red; all other types of actors are shaded in green.

PRODUCTS AND SERVICES ENABLING THIRD-PARTY BREACHES



The trend is clear: ransomware groups were responsible for all but one of the attributable attacks in our sample. Only one attack was attributable to a BEC scammer. Not a single one of the reported breaches in our sample was attributed to a state-sponsored group. The preeminence of ransomware groups among threat actors responsible for attributable attacks is a recurring theme in our reports. This insurance industry sample is nonetheless unusual in that ransomware groups dominate the sample so overwhelmingly, to the exclusion of other types of threat actors.

Equally important is the preeminence of C10p among the ransomware groups in our sample (43%). Its dominance is due to its massive mid-2023 campaign against users of the MOVEit file transfer software, which was a classic example of a third-party attack vector.

Ransomware operators often favor third-party attack vectors like MOVEit because they can infect many victims at once via one channel. To gain further insight into this correlation between ransomware and third-party attack vectors, we narrowed the sample of attributable attacks to those that

were also third-party breaches. Remarkably, this revised query removed only two attacks: the Nigerian BEC scam and an Everest ransomware attack with no third-party attack vector. All of the remaining attributable third-party breaches were ransomware attacks.

We attribute this correlation between third-party attack vectors and attributable ransomware attacks to a combination of factors. Ransomware attacks are often easier to attribute, given their use of distinctive proprietary payloads, and because operators must be able to fulfill publicly the threat of data disclosure that such attacks often include. Ransomware groups often prefer third-party attack vectors as a way to scale their operations. In contrast, more basic data breaches pose no such complications. Many other incidents in our sample fit this description, with no file encryption or data disclosure threats, no attributable actors, and no third-party attack vectors.

# Recommendations

## 1. Insurance Carriers Need More Comprehensive Third-Party Risk Management (TPRM)

Every insurance company should maintain a strong TPRM program, but carriers in particular need to prioritize it. Carriers depend on multiple lower-scoring segments of the industry, which increases their exposure to third-party cyber risk. Threat actors, including ransomware operators, often target the supply chain to bypass the stronger defenses of primary targets. This tactic makes carriers, which rely on weaker partners, especially vulnerable.

Prioritizing certain third parties can help carriers improve their security posture. General cross-industry software and IT providers should be at the top of the list, given their disproportionate role in third-party breaches. Insurance-specific software and IT vendors, as well as agencies & brokers, also warrant special scrutiny due to their lower scores and higher breach rates. Even partnerships with other carriers deserve attention, considering their higher frequency of breaches and compromised credentials—factors that amplify their third-party risk.

## 2. Ensure Your Vendors Have Their Own Effective TPRM Programs

Fourth-party breaches—those originating from your vendor's vendors—are an important but often overlooked risk. The MOVEit file transfer campaign showed that fourth-party breaches can occur even if your own defenses are sound. Reducing this risk means confirming that your direct vendors also manage their third-party risks. Merely vetting a vendor without assessing its supply chain leaves a gap that attackers can exploit.

## 3. Heightened TPRM for U.S. and Chinese Companies

Many organizations already take extra precautions when dealing with Chinese companies due to government-sponsored cyber activities. These measures remain wise and may need to be expanded. The unusually low scores of Chinese insurance companies add a second layer of risk—beyond any state-sponsored threats—that calls for additional safeguards.

At the same time, U.S. companies may pose greater third-party risks due to their popularity as targets and their high rates of compromised credentials. When working with U.S. partners, consider encrypting sensitive email communications and applying stricter controls.

## 4. Do Not Pay Ransoms to Ransomware Operators

We strongly discourage paying ransoms for several reasons. Legal risks may arise if you send money to sanctioned entities. Paying a ransom can also encourage more attacks by rewarding criminal behavior. Attackers may fail to restore your data, demand more money, or sell your information regardless of payment. Even if they try to restore your files, technical errors can result in permanent data loss. Avoiding ransom payments helps reduce the incentive for attackers and protects the broader ecosystem.

# CONCLUSION

SecurityScorecard's findings highlight persistent third-party and supply chain vulnerabilities, uneven performance across industry segments, and distinctive geographic and threat patterns. By focusing on the most at-risk relationships, ensuring vendors also manage their own suppliers, and refusing to fund criminal operations, organizations can bolster their overall security posture. Continuous monitoring, ongoing assessment, and informed decision-making remain essential to staying ahead of evolving threats—and SecurityScorecard stands ready as a resource to help insurance industry stakeholders achieve these goals.



To learn more and create  
your free account, visit  
[SecurityScorecard.com](https://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](https://securityscorecard.com) or connect with us on [LinkedIn](#).



[SecurityScorecard.com](https://SecurityScorecard.com)  
[info@securityscorecard.io](mailto:info@securityscorecard.io)