NAIC®

MEMORANDUM

Report on the Cybersecurity Insurance Market

For Members and Interested Regulators of the **Property and Casualty Insurance (C) Committee** and **Innovation Cybersecurity and Technology (H) Committees**

This report examines the cyber insurance market using data from the NAIC's *Property & Casualty Annual Statement Cybersecurity Insurance Coverage Supplement* (Cyber Supplement) and alien surplus lines data from the NAIC's International Insurers Department (IID). Formerly, the *Cybersecurity and Identity Theft Supplement* required U.S.-domiciled insurers to report the following information on cybersecurity insurance policies in either a stand-alone or packaged coverage manner:

- Number of claims reported (first- and third-party).
- Direct premiums written and earned.
- Direct losses paid and incurred.
- Adjusting and other expenses paid and incurred.
- Defense and cost containment expenses paid and incurred.
- Number of policies in force (claims made and occurrence).

Note that insurers were only required to file direct premiums written and earned for cybersecurity insurance coverage sold as part of a package policy if it was available or estimable.

Effective for the 2024 annual statement filings, the Cyber Supplement no longer requires reporting for identity theft-related information. Additionally, it has changed from a two-way stand-alone/packaged split to a three-way primary/excess/endorsement split.

"Packaged" was intended to mean where cybersecurity insurance was covered as an endorsement only. The change in wording from the NAIC is now a clear distinction between policies covering only cyber versus policies for which cyber is an endorsement to another policy. The three-way split results in a better picture of the types of policies being written and the premium paid for cybersecurity insurance coverage.

The overhauled Cyber Supplement creates state-level transparency for the first time since the NAIC began collecting data on cyber insurance.

The report discusses changes in the U.S. cyber insurance market and the cybersecurity landscape. It offers some reasons for these changes to help better understand the U.S. cyber insurance market, which remains the largest in the world.

Overview

Globally cyber insurance premiums reached nearly $15 billion in premium written for cybersecurity coverages in 2024, a 7% increase from the previous year.[1] Most of this growth occurred outside the U.S., where premiums were slightly lower.

The U.S. cyber insurance market witnessed its first ever reduction in Direct Written Premium (DWP), with approximately $9.14 billion written in 2024. This is a 7% decrease from 2023 which reported $9.84 billion including domiciled insurers and alien surplus lines carriers writing coverage throughout the market.

The U.S. domiciled insurers reported $7.08 billion in DWP, down slightly from the $7.25 billion in DWP reported for 2023. The number of policies in force decreased slightly (0.03%) from the year prior with 4,368,614 in 2024. The number of claims rose almost 40% with nearly 50,000 reported. Despite more incidents, Aon's U.S. broking clients saw average ransom payments drop by 77% in 2024, reflecting improved controls and negotiation.[2] As cyber-attacks persisted, the frequency of cyber claims grew across 2024, ranging from ransomware and business interruption to class action litigation and regulatory investigations, resulting in an increasingly complex incident response. For example, Aon Cyber and Errors and Omissions (E&O) claims data revealed 1,228 reported incidents across broking clients in 2024, reflecting an increase of 22% year over year.

Cyber insurance rates in the U.S. declined an average of 5% in the fourth quarter of 2024, marking the first quarterly decrease following seven years of rising rates.[3] As companies continued to invest in their cybersecurity controls, which is looked upon favorably by underwriters, many also sought to increase limits, reduce retentions, and make other program improvements. Cyber risk remains a top concern for organizations. Mitigating third-party-driven cyber incidents with widespread consequences, even non-malicious events such as the July 2024 CrowdStrike incident, may only increase in importance as companies continue to integrate more third-party solutions. [4]

Adversaries are running a business; cybercriminals are becoming highly efficient, using automation, artificial intelligence (AI), and advanced social engineering to scale attacks and maximize impact. 2024 saw a dramatic rise in malware-free intrusions, from vishing, which saw a 442% surge, to identity-based intrusions. Adversaries are more organized and effective than ever.[5] Help desk social engineering also surged, while nation-state actors expanded their operational tempo and global reach. In this dynamic environment, cyber insurance remains a vital component of risk management, helping organizations mitigate financial losses and recover from increasingly complex and high-velocity cyber incidents.

[1] https://www.insurancebusinessmag.com/reinsurance/news/breaking-news/cooling-cyber-reinsurance-continues-but-systemic-risks-and-ai-threats-loom--moodys-548969.aspx
[2] https://beinsure.com/global-cyber-risk-trends/
[3] https://www.marsh.com/en/services/cyber-risk/insights/cyber-insurance-market-update.html
[4] https://www.marsh.com/en/services/cyber-risk/insights/crowdstrike-software-update-outage.html
[5] https://www.crowdstrike.com/en-us/global-threat-report/

Report on the Cybersecurity Insurance Market

Market Penetration and Growth

FIGURE 1

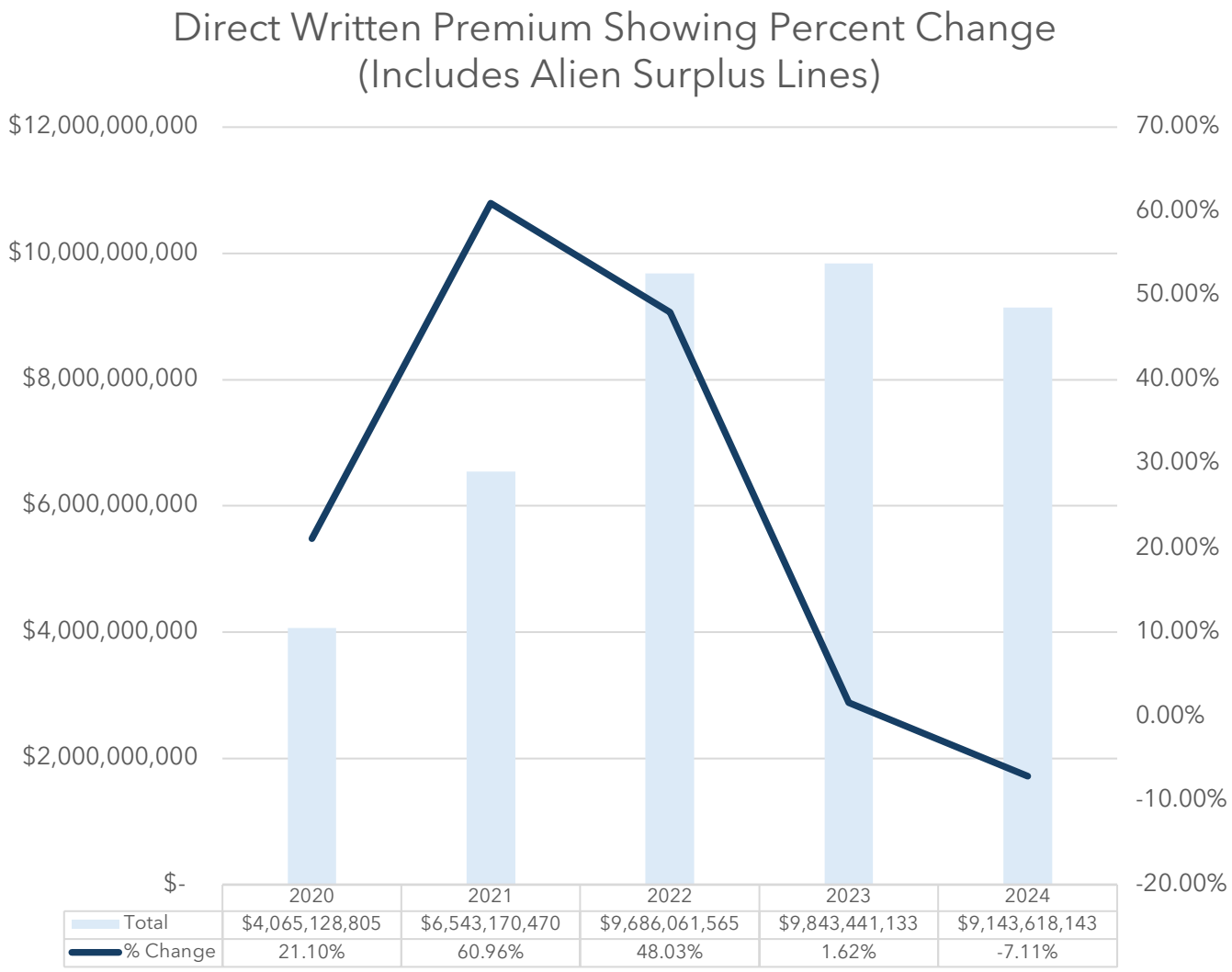
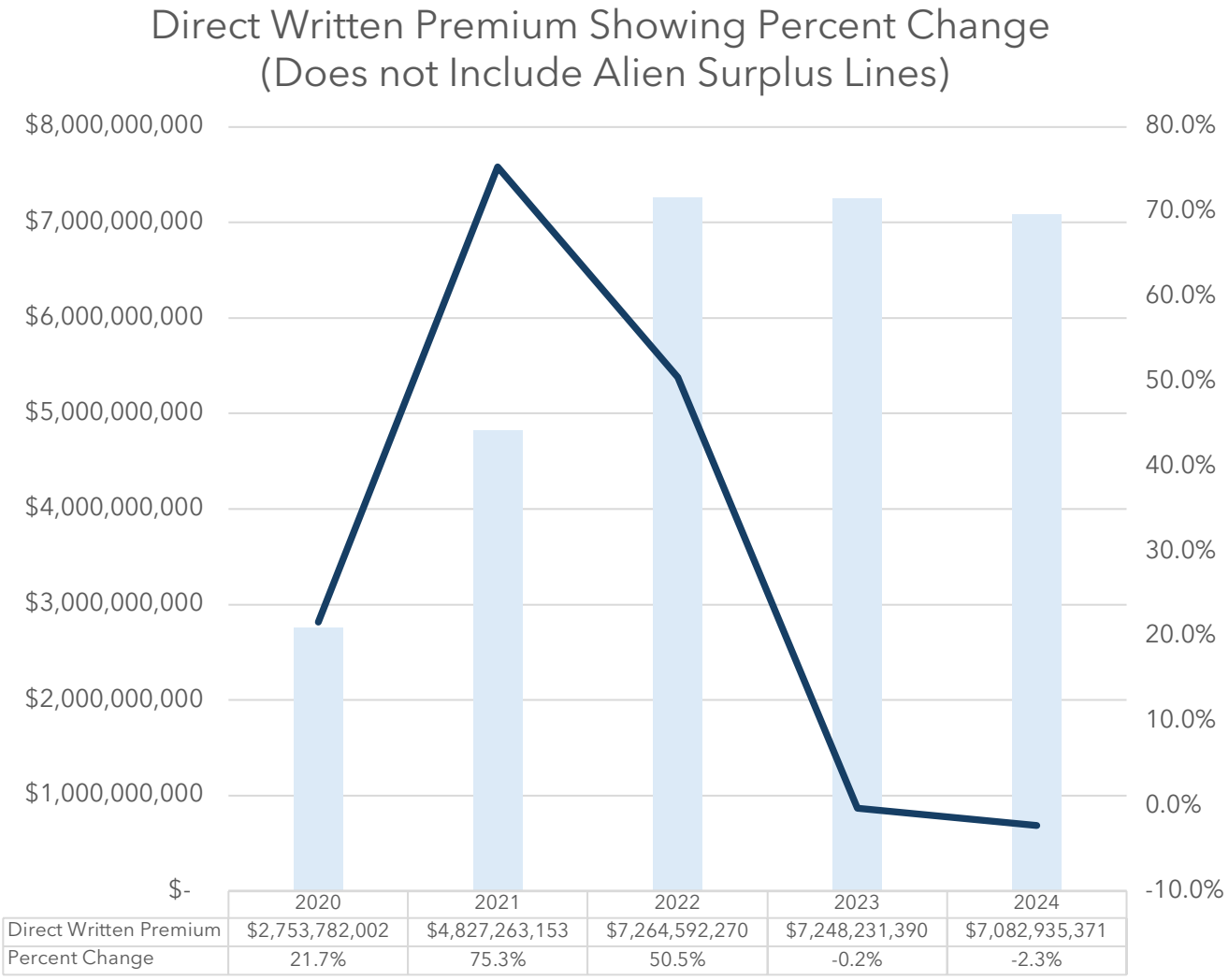


Figure 1 tracks the direct written premium (DWP), including alien surplus lines, from 2020 to 2024. The data illustrates a dramatic expansion from 2020 to 2022, with a peak year-over-year growth of nearly 61% in 2021. This period of rapid premium increases reflects the market's reaction to a more complex and volatile cyberthreat landscape. Following this surge, growth slowed significantly to 1.62% in 2023. The market then contracted for the first time in this period, declining by 7.11% in 2024.

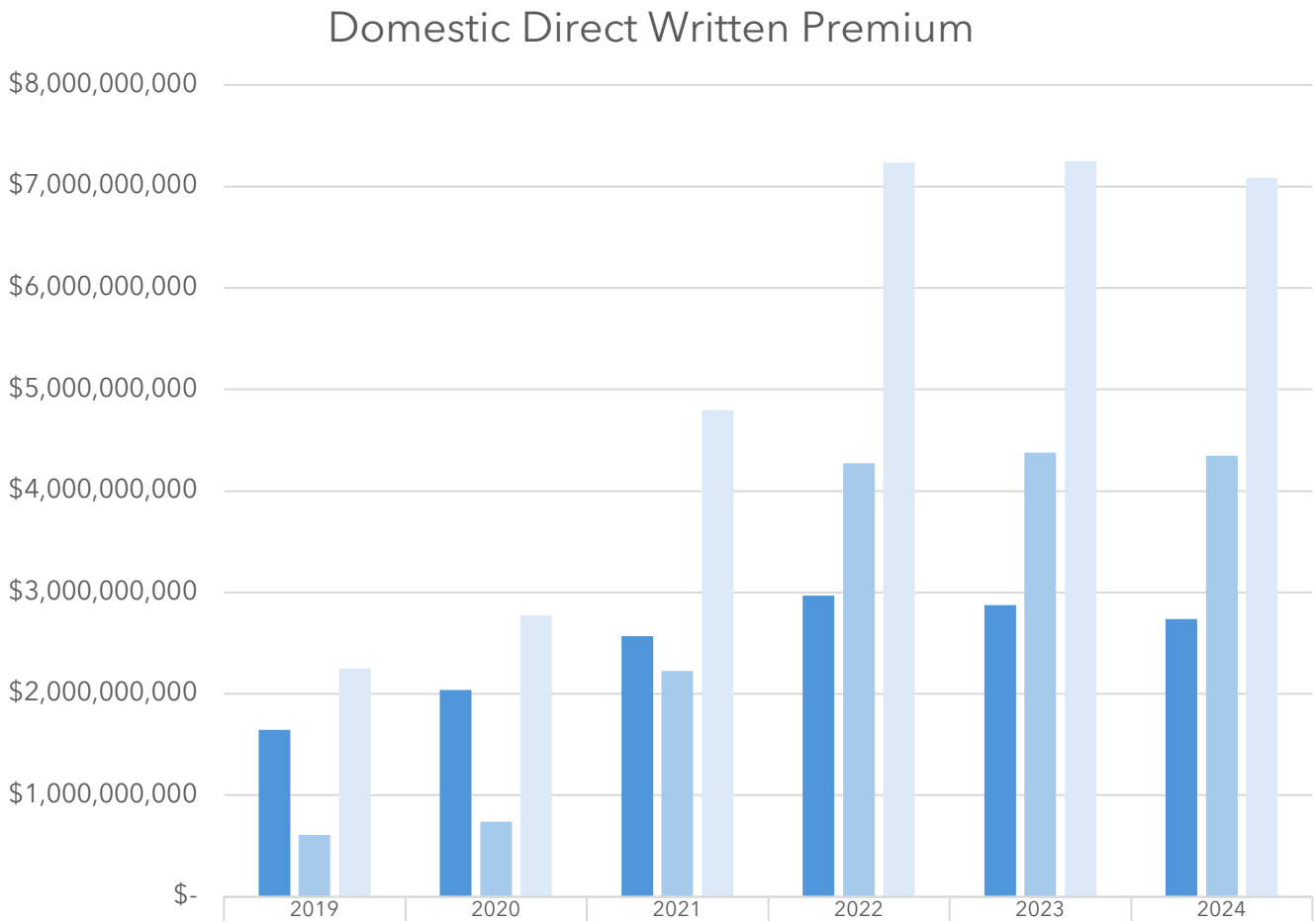
FIGURE 2



	2020	2021	2022	2023	2024
Direct Written Premium	$2,753,782,002	$4,827,263,153	$7,264,592,270	$7,248,231,390	$7,082,935,371
Percent Change	21.7%	75.3%	50.5%	-0.2%	-2.3%

Figure 2 presents the trend in DWP specifically for the U.S. domestic market, excluding alien surplus lines, from 2020 to 2024. The domestic market experienced even more aggressive growth than the total market, peaking at a 75.3% increase in 2021. The subsequent market stabilization was also more abrupt, with premium growth halting in 2023 (-0.2%). In 2024, the domestic market saw a modest 2.3% decline, indicating a more moderate contraction compared to the total market shown in Figure 1.

FIGURE 3



	2019	2020	2021	2022	2023	2024
Admitted DWP	$1,642,920,330	$2,036,258,695	$2,571,578,654	$2,966,506,950	$2,873,289,761	$2,737,173,810
Surplus Lines DWP	$609,758,664	$738,259,451	$2,224,187,581	$4,270,730,490	$4,374,941,629	$4,345,761,561
Total	$2,252,678,994	$2,774,518,146	$4,795,766,235	$7,237,237,440	$7,248,231,390	$7,082,935,371

Figure 3 represents the domestic direct written premium for the U.S market from 2019 to 2024.

FIGURE 4

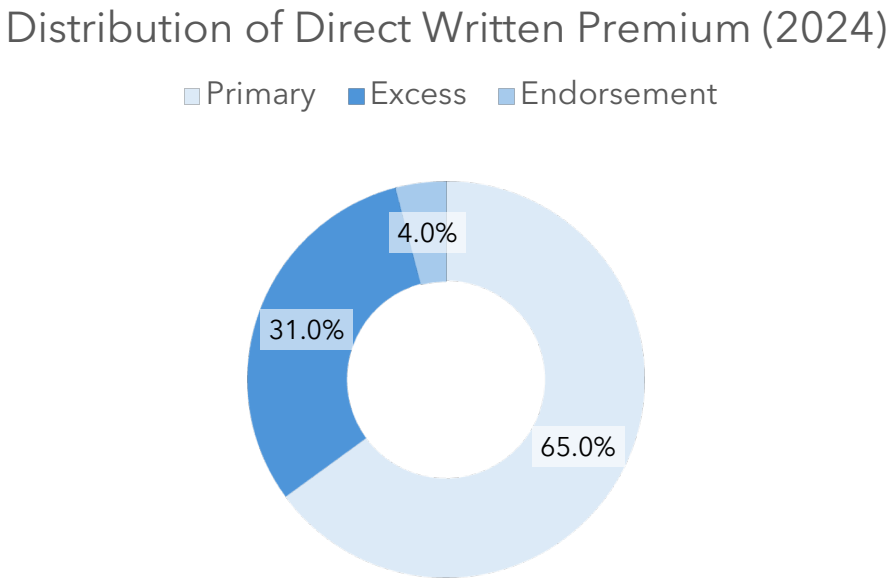


Figure 4 represents the 2024 market distribution of DWP across the three main policy structures. The chart indicates that primary policies generate the vast majority of the premium, accounting for 65% of the total. Excess policies are the second-largest contributor at 31%, while endorsement policies comprise the smallest segment at 4%. This distribution highlights that premium value is concentrated in the cyber insurance market.

FIGURE 5

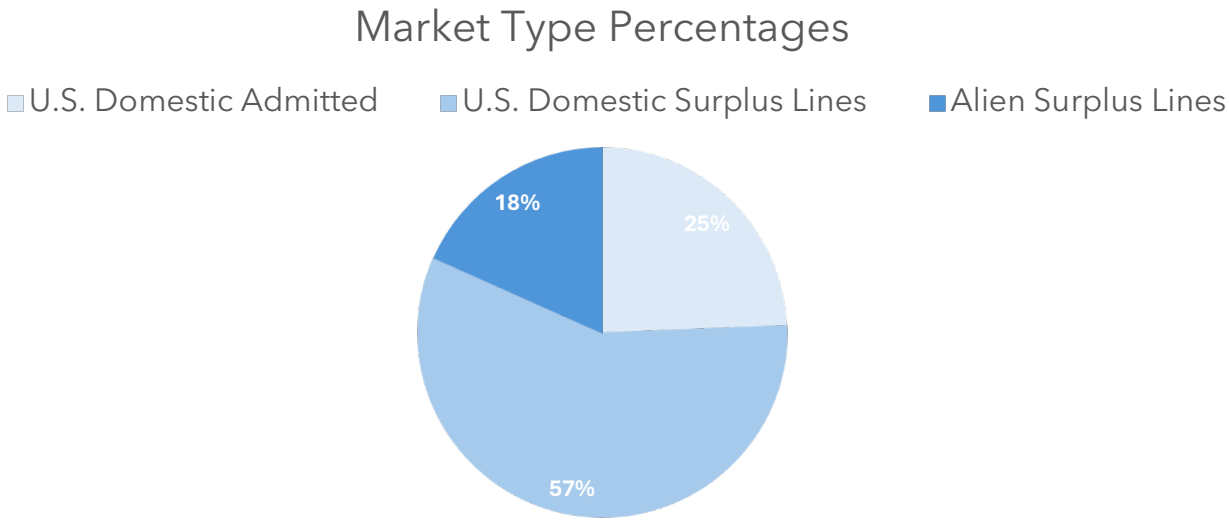


Figure 5 represents the U.S. market as shares of the total direct written premium for 2024, including admitted surplus lines, and alien surplus lines segments. Domestic surplus lines held 57% of the market share, an increase of 12% from 2023.

FIGURE 6

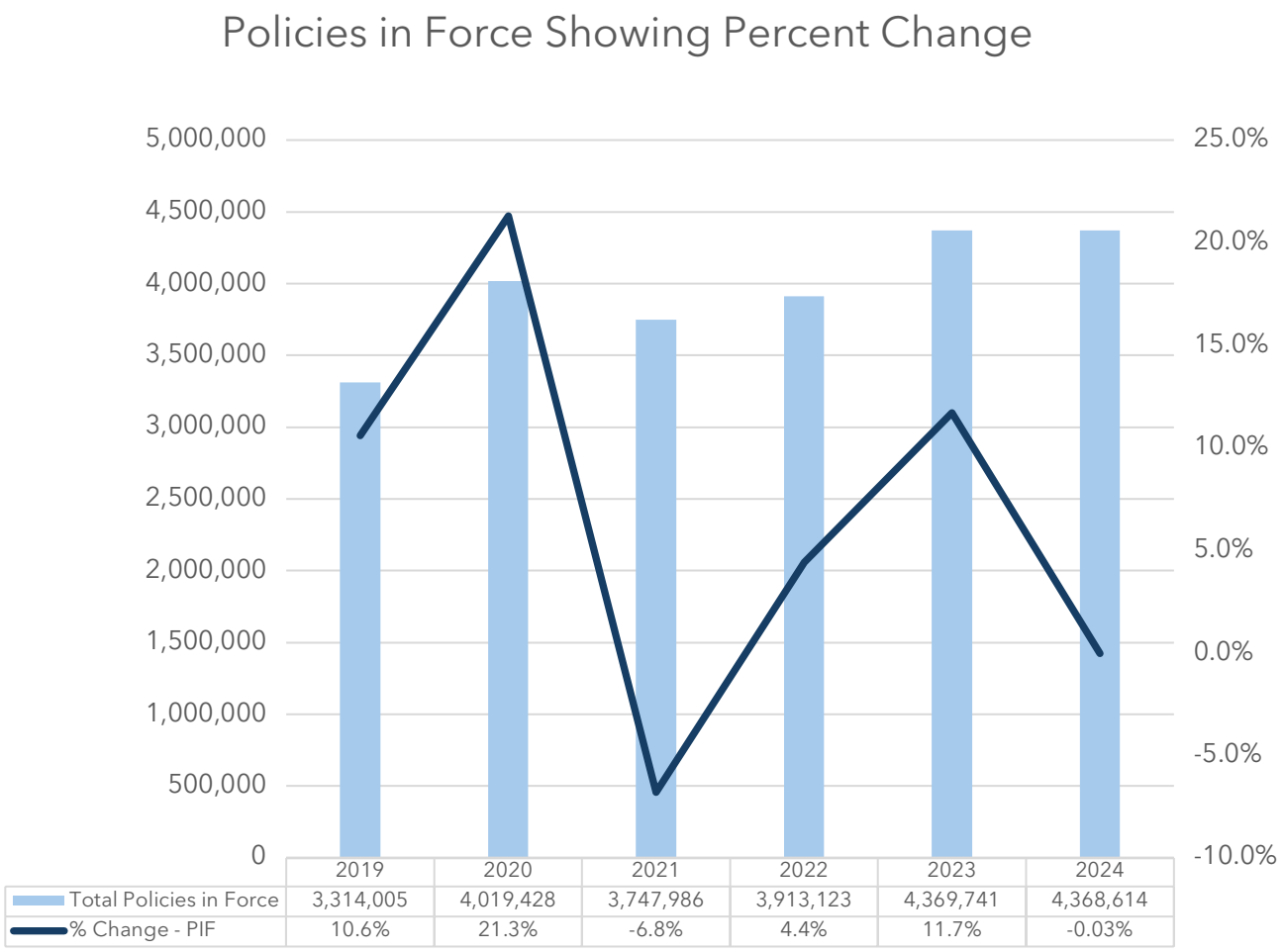


Figure 6 illustrates the total number of cyber insurance policies in force (PIF) and the annual rate of change from 2019 to 2024. After a period of strong growth, the market experienced a significant 6.8% decrease in total policies in 2021. Adoption rebounded strongly in the following years, with the number of policies growing 11.7% in 2023 to a new peak of nearly 4.4 million. However, this growth halted in 2024, with the number of active policies remaining flat (0.03% change). This plateau in policy count suggests that the market has reached a new stage of maturity in terms of customer adoption.

FIGURE 7

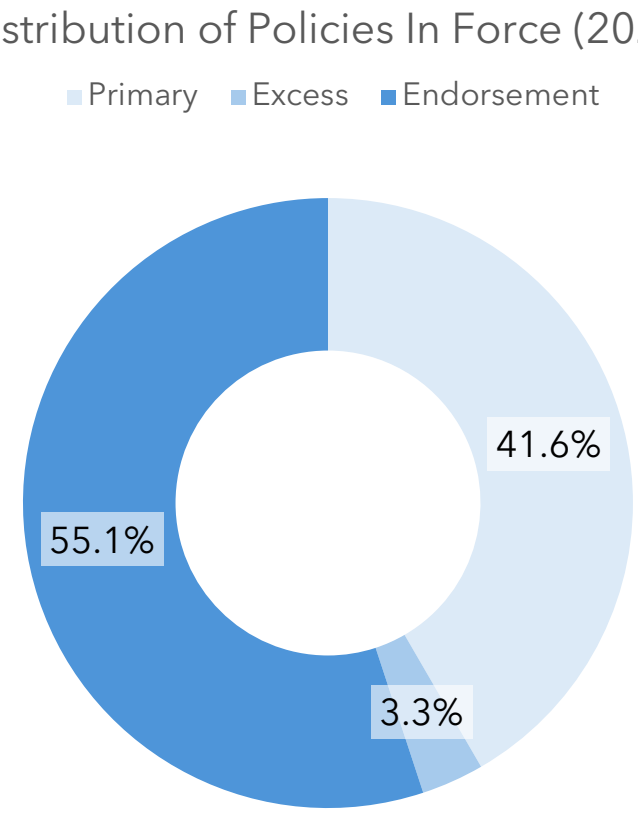


Figure 7 illustrates the distribution of PIF by type for 2024. In contrast to premium distribution, endorsement policies are the most numerous, comprising 55.1% of all active policies, followed by primary policies at 41.6%. Excess policies are the least common representing 3.3% of policies. Comparing this with the DWP distribution reveals a key market insight: Endorsement policies are high-volume but low-premium products, whereas excess policies are low-volume but high-premium products.

Table 1
Use the new Part 5 of the Cyber Supplement to analyze state-level distribution and identify geographic expansion or concentration for Table 1.

State	DWP	Share
DE	$1,182,868,526	17.69%
IL	$1,044,990,554	15.63%
CT	$863,009,514	12.91%
TX	$648,725,618	9.70%
PA	$574,626,360	8.60%
MO	$319,338,804	4.78%
OH	$301,713,683	4.51%
NH	$258,028,760	3.86%
NY	$254,990,091	3.81%
ND	$235,845,109	3.53%
FL	$180,668,825	2.70%
RI	$133,496,854	2.00%
NE	$126,631,690	1.89%
AZ	$115,603,134	1.73%
IA	$77,323,621	1.16%
IN	$64,338,599	0.96%
NJ	$57,188,267	0.86%
WI	$44,238,273	0.66%
CO	$28,595,430	0.43%
GA	$25,774,666	0.39%

Table 1 illustrates the state-level market share distribution based on DWP. The data reveals a significant concentration of the cyber insurance market within a small number of states. Delaware commands the largest market share with 17.69% of the total DWP, followed by Illinois (15.63%), Connecticut (12.91%), Texas (9.70%), and Pennsylvania (8.60%). Collectively these five states represent more than 64% of the entire U.S. market, indicating a notable geographic concentration of cyber insurance premiums.

Profitability and Risk Exposure

FIGURE 8

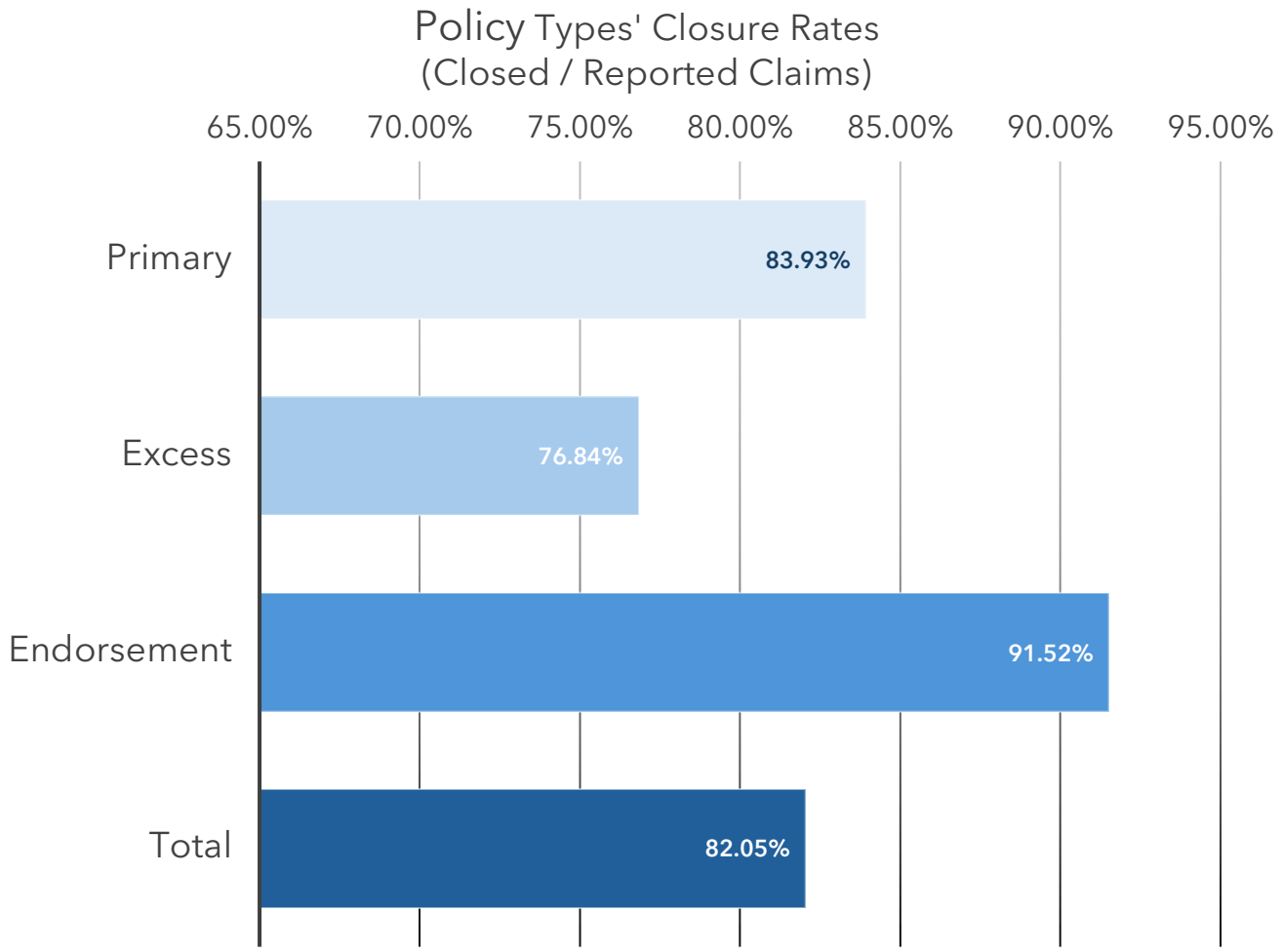


Figure 8 compares the claim closure rates and the percentage of reported claims that have been resolved across the different policy structures. The data shows that endorsement policies have the highest closure rate at 91.52%, indicating a greater efficiency or simplicity in resolving their associated claims. In contrast, stand-alone policies like primary and excess policies have lower closure rates of 83.93% and 76.84% respectively. The lower closure rate for excess policies suggests that these claims are often more complex and remain open for longer periods.

FIGURE 9[6]

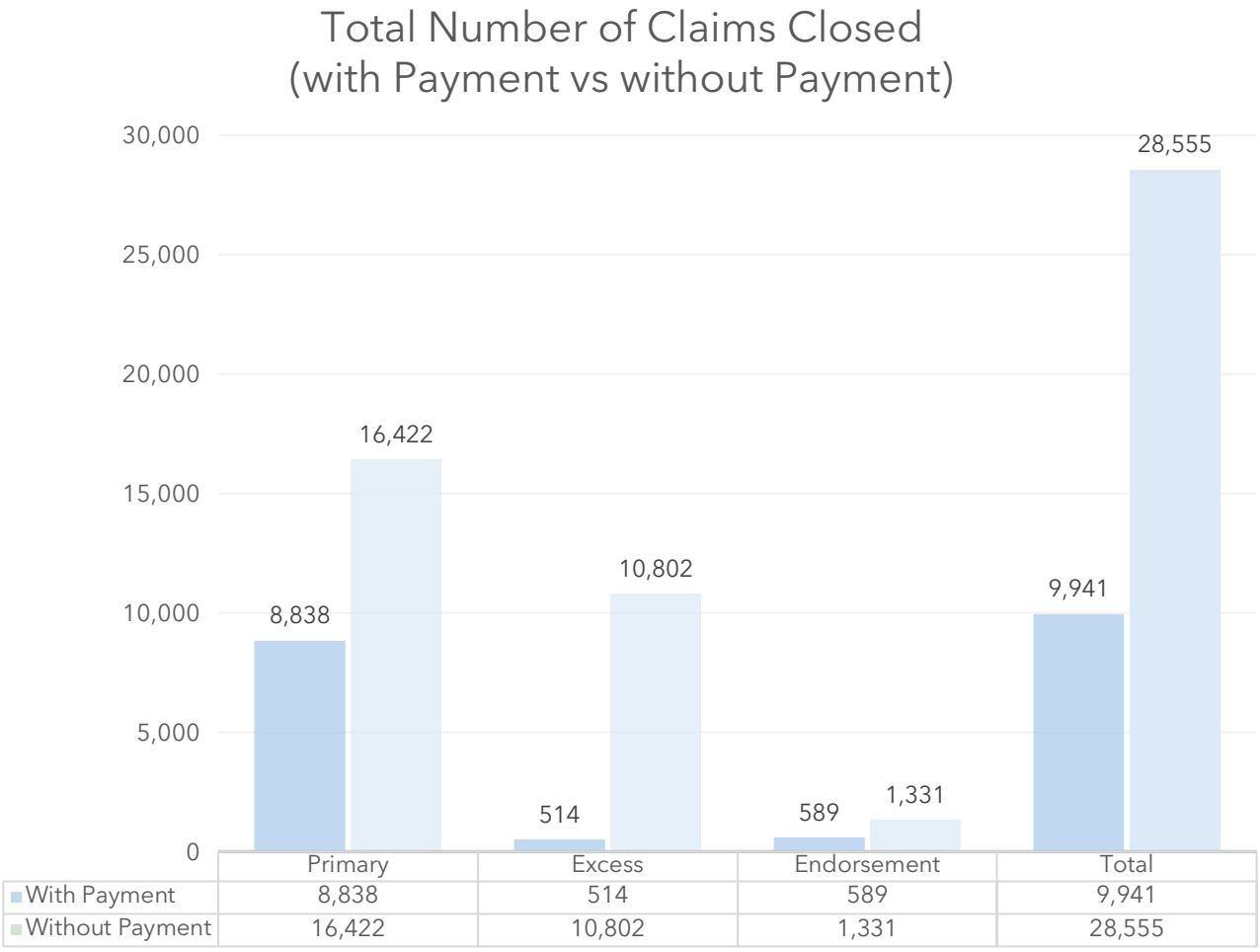


Figure 9 compares cyber insurance claims closed with payment versus those closed without one, categorized by policy structure. Across all types, the number of claims closed without payment (28,555) is nearly three times higher than those closed with a payment (9,941). This trend is consistent across all policy types but is most pronounced for excess policies, where claims are closed without payment outnumber paid claims by a ratio of more than 20-to-1.

[6] Does not include alien surplus lines.

Table 2- Top 20 Groups[7]

2024 Rank	2023 Rank	Group Name	Direct Written Premium	Loss Ratio with DCC	Market Share	Cumulative Market Share
1	1	Chubb Lt Grp.	$560,634,065	36.06%	7.92%	7.92%
2	4	St Paul Travelers Grp.	$535,426,655	53.97%	7.56%	15.48%
3	3	Fairfax Financial	$360,580,980	39.66%	5.09%	20.58%
4	5	Tokio Marine Holding Inc.	$355,982,823	43.47%	5.03%	25.60%
5	2	AXA Ins. Grp.	$340, 448,442	36.03%	4.81%	30.41%
6	7	Arch Ins. Grp.	$285,033,459	41.67%	4.03%	34.44%
7	32	At Bay Specialty Ins. Grp.	$280,601,661	55.78%	3.96%	38.40%
8	8	American Intrnl. Grp.	$276,564,105	49.26%	3.91%	42.31%
9	9	Sompo Grp.	$262,732,079	57.84%	3.71%	46.02%
10	10	Starr Grp.	$255,087,002	96.26%	3.60%	49.62%
11	11	CNA Ins. Grp.	$240,279,671	74.84%	3.39%	53.02%
12	14	AXIS Capital Grp.	$204,589,956	26.73%	2.89%	55.91%
13	18	AmTrust Financial Serv. Gr.	$202,476,467	48.33%	2.86%	58.77%
14	6	Berkshire Hathaway	$187,578,016	85.72%	2.65%	61.42%
15	16	Hartford Fire & Cas Grp.	$185,549,193	11.53%	2.62%	64.04%
16	19	Beazley Grp.	$184,854,545	9.24%	2.61%	66.65%
17	28	QBE Ins. Grp. Ltd.	$184,062,830	89.31%	2.60%	69.25%
18	15	Liberty Mut. Grp.	$169,793,294	70.72%	2.40%	71.65%
19	13	Zurich Ins. Grp.	$168,205,234	78.31%	2.38%	74.03%
20	17	Ascot Ins. US Grp.	$156,769,170	45.19%	2.21%	76.24%

Table 2 represents the direct written premium (DWP) and loss ratios for the top 20 insurer groups providing primary, excess, and endorsement policies in the cyber supplement.

[7] Does not include alien surplus lines.

Emerging Structures in Cyber Insurance Capacity

Reinsurance: The Hidden Engine

Reinsurance has played a pivotal role in expanding the capacity of the cyber insurance market.[8] Most reinsurance arrangements follow the primary insurance wording, typically through quota share agreements, with a growing use of excess of loss (XoL) structures. A significant portion of premium is ceded to a small group of global reinsurers, who aggregate claims and underwriting data from primary insurers.[9] This aggregation drives improvements in underwriting controls and policy wording. The sector has seen increased scrutiny of "silent cyber" exposures or unintended cyber risks embedded in non-cyber policies, which is prompting a push for clearer exclusions and contract language.[10]

Recent research shows that approximately 50-65% of global cyber premiums were ceded to reinsurance in 2022, highlighting reinsurers' pivotal role in sustaining market capacity.[11] Reinsurers increasingly diversify cyber risk across geography, technology, and industry while requiring higher transparency and portfolio data from primary insurers to control aggregation and capacity risks.[11]

Market-data indicates that the cyber reinsurance market is extremely concentrated: the top five reinsurers underwrite approximately 62% of cyber gross written premiums, and the top ten account for 87% of the market.[12] This level of concentration means that if one or more major reinsures withdraw or reduce cyber capacity, the ripple effects could be substantial for primary insurers and the broader market.

Cyber Warranties: Vendor-Backed Guarantees

Cyber warranties, often backed by technology vendors, offer narrow, tool-specific guarantees with strict preconditions. These products typically feature lower coverage limits and are sometimes supported by insurance carriers, though many warranties are never triggered.[13] Vendors leverage deep telemetry from their own technology stacks to inform risk, and qualifications often require rigorous operational and cybersecurity hygiene standards.[14] The first public cyber warranties emerged in the mid-2010s, with broader offerings targeting managed service providers (MSPs) following soon after.[10]

[8] https://academic.oup.com/cybersecurity/article/10/1/tyae027/7920185
[9] https://captives.insure/insights/cyber-reinsurance-market-and-trends
[10] https://academic.oup.com/cybersecurity/article/11/1/tyae028/7962043
[11] https://academic.oup.com/cybersecurity/article/10/1/tyae027/7920185
[12] https://www.reinsurancene.ws/howden-res-cyber-risk-report-reveals-62-market-share-held-by-top-5-reinsurers/?utm_source=chatgpt.com
[13] https://bawn.com/risk-resilience-bawns-guide-to-cybersecurity-and-beyond/the-rise-of-cyber-warranties-a-new-layer-of-protection
[14] https://www.beltexins.com/insights/the-three-types-of-cyber-warranties-and-associated-risks

Parametric Cover: Trigger-Based Payouts

Parametric insurance products in cyber pay out based on predefined events, such as General Data Protection Regulation (GDPR)-reported breaches or cloud region outages, rather than the actual size of the loss. These covers are characterized by tight limits, objective triggers, and are often backed by reinsurers.[15] Independent monitoring of service providers and public registries is used to verify triggers, enabling fast and certain payouts. The first multi-peril parametric covers appeared in 2019, with subsequent expansion into broader cloud outage scenarios.[16]

Capital Markets: Catastrophe Bonds and Investor Capacity

The entry of capital markets into cyber insurance has introduced catastrophe (cat) bonds and other investor-backed instruments. These products, which may be tied to indemnity, industry indices, or parametric triggers, are still a small but growing part of the market.[17] Investors assess catastrophe models and the quality of insurers' portfolios before participating. The influx of outside capital supports disciplined underwriting and strong risk controls. The first dedicated cyber cat bond was issued in 2023, with additional issuances in 2024.[18]

Market Cycle Dynamics and Growth Outlook

Recent analysis of the global cyber insurance market reveals a pivotal shift in the market cycle after a period of rapid premium growth and hardening rates. The sector has entered a phase of rate softening and slower topline expansion. According to Howden, global cyber insurance rates have declined by 22% from their mid-2022 peak, and annual premium growth has slowed to 6% (2022–2024), down from the nearly 40% compound annual growth rate seen during the hard market of 2020–2022. Despite this moderation, underwriting profitability remains robust, with combined ratios averaging 70% and strong cumulative profits reported.[19]

[15] https://www.parametrixinsurance.com/solutions-cloud
[16] https://www.insurancejournal.com/news/international/2022/03/08/657170.htm
[17] https://www.genevaassociation.org/sites/default/files/2024-12/cyber_ils_report_1213.pdf
[18] https://cyberinsurancenews.org/cyber-catastrophe-bonds-growth/
[19] https://www.howdengroupholdings.com/reports/2025-cyber-report

Cybersecurity Threat Landscape

The *2025 Verizon Data Breach Investigations Report* (DBIR) analyzed more than 22,000 security incidents and more than 12,000 confirmed data breaches, representing the highest volume ever reviewed in a single year. Ransomware remains the most disruptive threat, present in 44% of breaches. While the median ransom paid decreased, the proportion of organizations refusing to pay increased to 64%, indicating improved resilience but persistent risk.[20] Professional ransomware negotiators can reduce payments by 64% and avoid payment in 70% of cases. [21]

With several groups striving to make a name for themselves in extortion circles, pushing boundaries seemed to be the focus of the ransomware landscape. Rapid7 Labs data saw 33 new or rebranded threat actors appearing between Jan. 1 and Dec. 10, 2024, according to their annual threat landscape statistics. [22] Groups like RansomHub exfiltrated data from hundreds of targets spanning healthcare, financial services, critical manufacturing, and many others by operating as a ransomware-as-a-service (RaaS) provider. The Cybersecurity and Infrastructure Security Agency (CISA) described how the affiliates leverage a double-extortion model by encrypting systems and exfiltrating data to extort victims.[23] It should be noted that data exfiltration methods are dependent on the affiliate conducting the network compromise and the ransom note dropped during encryption does not generally include initial ransom demand or payment instructions. Rather, the note often provides victims with a client ID and instructs them to contact the ransomware group via a unique URL reachable through the Tor browser.

Business email compromise (BEC) remains an underestimated cyber threat. While ransomware and supply chain attacks often dominate headlines, BEC has become one of the most financially damaging cyber threats facing organizations today. According to the Federal Bureau of Investigation (FBI), BEC attacks have resulted in more than $17 billion in reported losses in the U.S. alone over the past decade, with the average loss per incident now exceeding six figures.[24] Unlike technical exploits, BEC leverages social engineering and psychological manipulation to trick employees into transferring funds or divulging sensitive information. The frequency and sophistication of these attacks continue to rise, impacting organizations of all sizes and sectors, and driving a significant share of cyber insurance claims.

[20] https://www.verizon.com/business/resources/reports/dbir/
[21] https://arcticwolf.com/resource/aw/us-rp-cyber-insurance-outlook
[22] https://www.rapid7.com/blog/post/2024/12/16/2024-threat-landscape-statistics-ransomware-activity-vulnerability-exploits-and-attack-trends/
[23] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
[24] https://www.ic3.gov/PSA/2024/PSA240911

Credential Abuse and Infostealers

The first half of 2025 saw a surge in credential abuse and information-stealing malware activity, marking a new era in cybercrime dominated by organized criminal groups. According to Flashpoint's latest threat intelligence, there has been an 800% increase in stolen credentials, with 1.8 billion credentials compromised by infostealers. There has also been a 235% rise in data breaches leading to the exposure of 9.45 billion records, two-thirds of which occurred in the U.S. Notably, unauthorized access accounted for nearly 78% of breach incidents, underscoring the central role of credential abuse in today's threat landscape.[25]

Infostealers are malware designed to harvest login credentials, cookies, and sensitive data; they have become the initial access weapon of choice for cybercriminals. Their low cost, accessibility, and effectiveness have fueled a dramatic rise in identity-based attacks, enabling threat actors to penetrate organizations and their supply chains with ease. The proliferation of cybercrime-as-a-service operations, such as Katz Stealer and Atlantis AIO, has further democratized credential theft, allowing even low-skilled attackers to compromise thousands of accounts for as little as $30.[26] Dark web-based marketplaces for nefarious service providers have continued to increase in availability. Cybercriminals purchase IDs, financial accounts, and other financial and personal data from wholesalers who distribute stolen data directly or via affiliates for profit.[27]

Recent research from the Marsh McLennan Cyber Risk Intelligence Center, in partnership with Searchlight Cyber, provides compelling evidence that dark web exposure is a statistically significant predictor of cyber insurance losses.[28] Organizations with any data or mention on the dark web are more likely to suffer a cyber-attack and file a cyber insurance claim. Based on their study, organizations and insurers could use intelligence tools to identify where and how an organization is mentioned or targeted. Visibility into dark web exposure provides a window for proactive defense before a breach occurs.

Third Party and Supply Chain Risk

Third-party and supply chain risks have become a central concern in cyber insurance, with attackers increasingly bypassing direct defenses to exploit vulnerabilities in vendors, suppliers, and service providers. In 2024, 35.5% of all data breaches originated from third-party compromises.[29] The retail, hospitality, technology, and energy sectors are especially exposed, with more than 45% of breaches in these industries linked to third-party vendors. File transfer software and cloud services are among the most common enablers for supply chain attacks, and ransomware groups and state-sponsored actors, particularly from China, are the most prolific threat actors. The modern business ecosystem is so interconnected that a single compromise can cascade across multiple organizations.

[25] https://www.flashpoint.io/resources/report/flashpoint-global-threat-intelligence-index-midyear/?CRO2=232016_variant&CRO3=233007_control
[26] https://www.forbes.com/sites/daveywinder/2025/08/01/information-stealing-machine-behind-theft-of-18-billion-credentials/
[27] https://cymulate.com/blog/dark-web-shopping-center/
[28] https://slcyber.io/whitepapers-reports/the-correlation-between-dark-web-exposure-and-cybersecurity-risk/
[29] https://securityscorecard.com/resource/global-third-party-breach-report/

Human (Carbon) Element

Despite advances in cybersecurity technology, the most persistent vulnerability in 2025 remains the human factor. According to the Verizon DBIR, the human element is involved in 60% of all breaches. This includes social engineering, user error, and privilege misuse, underscoring that attackers increasingly exploit psychology rather than code.

Social engineering attacks leverage cognitive biases such as fear, urgency, authority, and curiosity. These tactics bypass technical defenses by manipulating individuals into granting access or transferring funds. The rise of artificial intelligence (AI) has amplified this risk: generative AI enables attackers to create sophisticated phishing emails and deploy hyper-realistic deep-fake audio/video, eroding trust in digital communication. [30]

The financial impact of human-driven compromises is escalating. BEC losses exceeded $2.77 billion in 2024, while phishing remains a leading initial attack vector linked to ransomware and fraud. Vishing and smishing campaigns have surged dramatically, and AI-generated phishing emails achieve significantly higher engagement rates than traditional attempts. Deepfake-enabled fraud cases, such as the $25.6 million Arup incident, highlight how identity trust can be weaponized at scale.[31]

Summary

The 2024 cyber insurance market reflects a transitioning sector, shaped by evolving threats and innovations in risk transfer. After years of rapid premium growth, the market has entered a period of adjustment, with the first recorded decline in U.S. direct written premium (DWP). Despite this moderation, cyber insurance remains a critical tool for organizations facing an increasingly complex and high-velocity threat environment. Driven by ransomware, business email compromise (BEC), and credential abuse, the frequency and severity of claims continue to challenge insurers and insureds. The rise of malware-free intrusions and artificial intelligence (AI)-powered social engineering underscores a need for adaptive risk management.

Innovations have expanded coverage options and introduced new mechanisms for managing systemic and emerging risks. Market capacity and resilience have been bolstered by reinsurance, vendor-backed cyber warranties, parametric covers, and the entry of capital markets through catastrophe bonds. At the same time, the sector faces heightened scrutiny over silent cyber exposures and the adequacy of policy language, prompting ongoing improvements in underwriting and contract clarity.

As cyber threats grow in sophistication and scale, the importance of robust cybersecurity controls, proactive incident response, and informed risk transfer strategies has never been greater. The data shows that direct losses to organizations remain a primary driver of claims, and that human factors like social engineering, user error, and privilege misuse are central to the risk landscape. The cyber insurance market is expected to evolve in response to technological advances, regulatory developments, and the persistent adversarial ingenuity. Stakeholders must remain vigilant, leveraging data-driven insights and collaborative approaches to safeguard against the next generation of cyber risks.

[30] https://deepstrike.io/blog/social-engineering-statistics-2025
[31] https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/