

Bloomberg Intelligence

Cyberattacks Offer Growth Market for Insurers

Read Research Report: Insurers' Cyber Opportunity Knocks



Kevin Ryan
Team: Insurance
BI Senior Industry Analyst



Charles Graham
Team: Insurance
BI Senior Industry Analyst

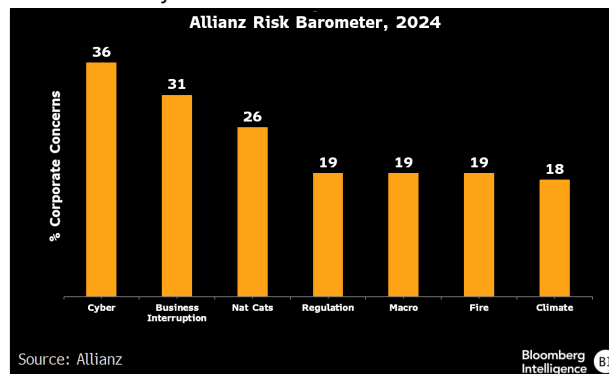
Cyber Insurer Market Demand May Rise as New Threats Emerge

(Bloomberg Intelligence) -- Demand for cyber insurance is set to grow amid a spate of high-profile attacks, with pioneer cyber-insurance provider Beazley (22.3% of 1H insurance contract written premiums) seeing 18% compound annual growth for that cover in 2024-30. Hiscox, Axis Capital, Chubb and Munich Re also see rising demand after the Change Healthcare attack in February and Ticketmaster's compromised 560 million customer records in May. (10/04/24)

1. \$8 Trillion Cyber Crime Cost Is an Insurer Opportunity

United Healthcare's Change Healthcare medical billing processor, which links one third of Americans to health-insurance payments, suffered a cyber attack in February, crippling the payments systems of a significant number of hospitals. The May attack on Ticketmaster compromising 560 million customer records is a further example of the unrelenting cyber-crime challenge. An estimated \$8 trillion was lost globally to cybercrime in 2023, according to technology consultants Cyber Security Ventures, a significant increase vs. the \$600 billion McAfee estimated in 2018. It's clear the seriousness of attacks is increasing. Allianz has said that cyber risk is the No. 1 concern globally, along with business interruption. (10/04/24)

Cyberattacks the No. 1 Concern

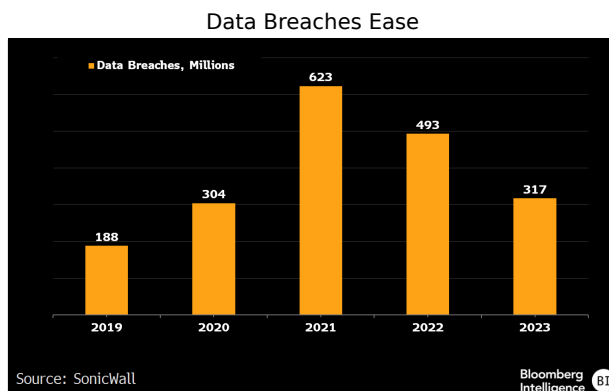


2. Ransomware Attack Volumes Decline; Insurers May Benefit

Following more than 317 million ransomware attacks globally in 2023 (2022: 493 million, 2021: 623 million), consultant Sonicwall monitored a 36% decline year-over-year globally, a one third fall in the US and Europe but an 11% rise in global malware attacks. The declines reflect both slowing economic activity and wins against ransomware perpetrators. Though insurers saw strong rises in cyber-insurance premium rates in 2022, these are now slowing, with Beazley's 2023 cyber rates falling 5% following a 40% rise in 2022. In mature markets, such as the US and Europe, cyber insurance may be one of the few areas of insurance to record real growth.

Cyber insurers Beazley, Hiscox, Axis, Munich Re and others could see more clients seek specialized cyber cover. (10/03/24)

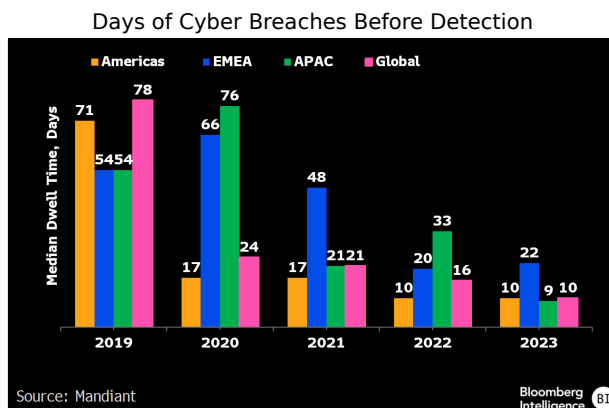
Bloomberg Intelligence



3. Cyber Risk Becoming a Headache for Many

Insurers have the infrastructure to work collaboratively with clients and provide services before and after malware incidents, thus minimizing potentially negative outcomes. Cyber threats and infiltration techniques are moving to more sustained levels -- known as "advanced persistent threats" -- away from quick, one-off acts. In these cases, criminals gain unauthorized access to computer networks and remain undetected. Activities can involve snatching a company's data for later use, or planning larger offensives. Mandiant (M-Trends 2024) reports that 17% of breached clients (27% in 2022) had more than one threat group in 2023.

The 2021 Mandiant figures show that pandemic-induced working from home didn't increase the number and severity of attacks or extend "dwell" times. (10/03/24)



4. Cybercrime Isn't About Tech: It's About People

Cyberattacks feature increasingly complex technology to circumvent firewalls, anti-virus software and other security protections, yet their success nevertheless often involves help from unsuspecting employees within the target companies. Financial institutions are the favored prey, though criminals have broad tastes when it comes to their potential victims.

IBM (Security X-Force Threat Intelligence Index) found that the most common attacks involve emails, with 30% of attacks using phishing directly tied to employee error. Another 30% of attacks came from abuse of valid account details sourced from the dark web. This was the third most common attack form in 2023. (10/03/24)

This report may not be modified or altered in any way. The BLOOMBERG PROFESSIONAL service and BLOOMBERG Data are owned and distributed locally by Bloomberg Finance LP ("BFLP") and its subsidiaries in all jurisdictions other than Argentina, Bermuda, China, India, Japan and Korea (the "BFLP Countries"). BFLP is a wholly-owned subsidiary of Bloomberg LP ("BLP"). BLP provides BFLP with all the global marketing and operational support and service for the Services and distributes the Services either directly or through a non-BFLP subsidiary in the BLP Countries. BFLP, BLP and their affiliates do not provide investment advice, and nothing herein shall constitute an offer of financial instruments by BFLP, BLP or their affiliates.

Bloomberg Intelligence

Favored Targets of Cyber Criminals

Top 10 Industries	2020 Rank	2021 Rank	2022 Rank	2023 Rank
Finance, Insurance	1	2	2	2
Manufacturing	2	1	1	1
Energy	3	4	4	4
Retail	4	5	5	5
Professional Services	5	3	3	3
Government	6	8	8	7
Healthcare	7	6	7	6
Media	8	10	10	10
Transport	9	7	9	8
Education	10	9	6	9

Source: IBM

Bloomberg Intelligence BI

5. Ransomware Events a Greater Problem

Ransomware attacks have become ubiquitous, with the dark web supplying platforms for these activities making the further case for insurers to cover seemingly unavoidable events. The latter are increasingly sophisticated, with bolder attacks that can leave businesses in danger of not having access restored to their own systems even after ransom payments. The Chainalysis 2024 Crypto Crime Report shows that 2023 was a record year with \$1.1 billion paid to ransomware attackers (double the 2022's \$500 million), citing a substantial increase in the scope and complexity of attacks.

Some attackers also allegedly place "Trojans" into the hacked systems to steal data at a later date. (10/03/24)

Preventing Ransomware Attacks

Five Ways to Prevent Ransomware	
Training	Help staff recognize phishing attacks
Back-Ups	Back-ups to prevent malware spreading
Lock Down RDP	Close remote desktop ports or
Multi-Factor Authentication	Use RDP & good practices everywhere
Patching, Anti-Virus	Keep all systems up to date

Source: Bloomberg Intelligence

Bloomberg Intelligence BI

6. Accidental Breaches May Spur Insurance Buys

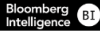
New regulations -- such as the 2018 EU General Data Protection Regulation (GDPR) or California's Consumer Privacy Act -- insist that companies do more to protect personal data collected from consumers. Accidental leaks or hacks put these companies at risk for legal repercussions and damaged reputations. Significant fines have been imposed, with 1.6 billion euros in the year to August 2023 a sharp year-over-year rise according to Data Privacy Manager, which could motivate greater business interest in insurance coverage. Fines levied in Europe under GDPR can see penalties charged of up to 4% of a company's annual global turnover. Repeated fines would likely see a company's Directors and Officers insurance as well as other insurance covers rise. (10/03/24)

This report may not be modified or altered in any way. The BLOOMBERG PROFESSIONAL service and BLOOMBERG Data are owned and distributed locally by Bloomberg Finance LP ("BFLP") and its subsidiaries in all jurisdictions other than Argentina, Bermuda, China, India, Japan and Korea (the "BFLP Countries"). BFLP is a wholly-owned subsidiary of Bloomberg LP ("BLP"). BLP provides BFLP with all the global marketing and operational support and service for the Services and distributes the Services either directly or through a non-BFLP subsidiary in the BLP Countries. BFLP, BLP and their affiliates do not provide investment advice, and nothing herein shall constitute an offer of financial instruments by BFLP, BLP or their affiliates.

Bloomberg Intelligence

Violations in Europe

2023-24 GDPR Fines	Euro Million	Date
Meta	1200	May-23
Meta	390	Sep-23
TikTok	345	Sep-23
Criteo	40	Jun-23
Enel	79	Feb-24
Amazon France	32	Jan-24
Avast Software	14	Apr-24

Source: Secure Privacy 

To contact the analyst for this research:
Kevin Ryan at kryan119@bloomberg.net