RISK & REGULATION

Insurers revisit cyber coverage as demand, premiums spike

Thursday, July 7, 2022 3:23 PM ET

By Tom Jacobs and Hassan Javed
Market Intelligence

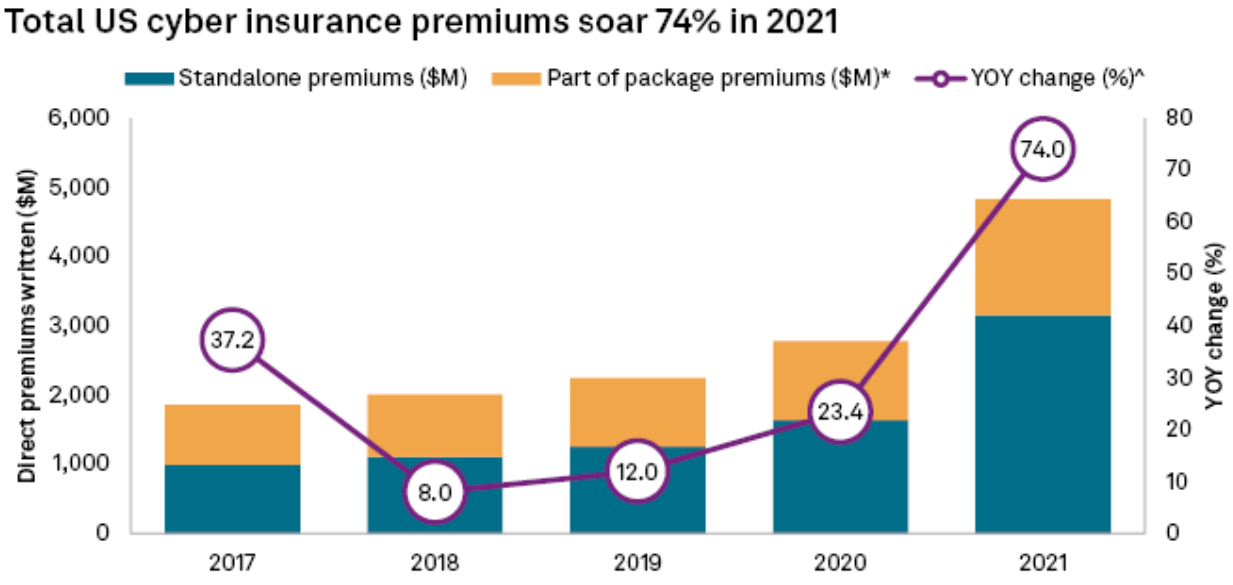
U.S. insurers are reevaluating their approach to cybersecurity cover as increasingly common ransomware attacks push premiums higher and ratchet up demand for coverage.

The frequency of ransomware events between 2018 and 2020 quadrupled, according to Rachel Rossini, underwriting manager for cyber for AXA XL, who said those events were "about 1,000% more severe."

According to a report from the CyberEdge Group, an IT research firm, 89.7% of organizations in the U.S. experienced at least one cyberattack in 2021, up from 78.5% a year earlier. Rossini said this rise in ransomware attacks has led to Axa XL "re-underwriting our entire book" as the company gets in tune with their clients' cybersecurity needs.

Premiums skyrocketing

The higher-risk environment has resulted in written premiums for all cyber policies jumping to $4.61 billion in 2021, a 74.1% year-over-year increase from $2.65 billion in 2020, according to an S&P Global Market Intelligence analysis. Premiums for stand-alone cyber policies spiked 92.3% to $3.15 billion in 2021 from $1.64 billion in the prior year, while cyber coverage included in policy packages spiked 44.7% to $1.46 billion from just over $1 billion in 2020.



Data compiled June 30, 2022.
* Includes both quantified and estimated direct premiums written.
^ Value shown is based off of the year-over-year change of total cyber insurance direct premiums written.
Data reflects the aggregation of all individual property and casualty filers that submit regulatory statements to the NAIC. Based on direct premiums written reported within annual NAIC statutory property and casualty filings: Cybersecurity and Identity Theft Insurance Coverage Supplement Part 2 – Stand-Alone Policies and Part 3 – Part of a Package Policy. U.S. filers only but may include business written outside the U.S.
Source: S&P Global Market Intelligence

Rossini said rate increases in 2022 have averaged "above 100%" compared with 2021, increases that were not necessarily spurred simply by higher demand.

"It has more to do with just the supply and the willingness of insurers to put up limits and the amount of premium we need to charge for it to sustain the losses we've been seeing," Rossini said.

Bob Wice, Beazley PLC's head of underwriting management for cyber, said the premium surge began after the market started to change due to a drop in capacity in late 2020.

"Insurers were starting to realize that they were getting hit in a way that they'd never been before with these types of ransomware events," Wice said in an interview. "So pricing and demand were up because there were a lot of public reports about organizations getting hit with ransomware attacks."

The cyber market continues to wrestle with "unsustainable" rates and an influx of new, inexperienced carriers, Rossini said, adding that there was a lack of "nuanced underwriting" in the market.

Cyber premium prices increased by an average of 27.5% in the first quarter of 2022, according to a report from the Council of Insurance Agents and Brokers. The report also cites an analysis by the Computing Technology Industry Association, which found that the cost of cyber claims increased by 10% in 2021, and the average cost for a data breach came in at more than $4 million.

Ukraine war impact

An increase in Russia-based cyberattacks is one of the outgrowths of the invasion of Ukraine. A report published by Microsoft Corp. said it had detected 128 organizations in 42 countries other than Ukraine that had been subjected to Russian network intrusion efforts, with the U.S. being the top target.

Microsoft President Brad Smith said in the report's introduction that while governments have been the primary targets for Russian entities, they have also focused on think tanks, humanitarian organizations, IT firms and critical infrastructure suppliers. The attacks Microsoft monitored had a 29% success rate, but that number "likely understates the degree of Russian success," Smith said.

Largest US cyber insurers in 2021

Market share (%)	Insurer	Direct premiums written ($M)	2020 to 2021 YOY premium change (%)
9.8	Chubb	473.1	17.1
9.0	Fairfax Financial	436.4	302.1
8.7	AXA SA	421.0	43.7
5.2	Tokio Marine	249.8	189.3
5.0	AIG	240.6	5.3
4.8	Travelers	232.3	12.3
4.2	Beazley PLC	200.9	13.0
3.8	CNA	181.4	51.6
3.5	Arch Capital	171.2	967.3
3.3	AXIS	159.1	19.1
42.7	All others	2,061.5	106.1

Data compiled June 24, 2022.
Based on stand alone and total package cyber insurance premiums reported within annual NAIC statutory property and casualty filings: Cybersecurity and Identity Theft Insurance Coverage Supplement Part 2 – Stand-Alone Policies and Part 3 – Part of a Package Policy. U.S. filers only but may include business written outside the U.S. Excludes certain New-Jersey domiciled subsidiaries that do not file quarterly statements with the NAIC because of state regulations.
The insurers in this analysis include groups that represent the consolidation of data of the statutory filers within SNL-defined group structures and unaffiliated single companies.
Source: S&P Global Market Intelligence

The war has not had a serious effect on claims for AXA XL, which is the third-largest cyber insurer in the U.S., behind Chubb Ltd. and Fairfax Financial Holdings Limited and ahead of Tokio Marine Holdings Inc. and American International Group Inc. Even still, Rossini said the company has taken "proactive underwriting actions" such as network segregation to ensure that any action taken against one network does not affect others around the world.

"A lot of our clients that have shut down a lot of their operations in Russia or Ukraine ... have been winding down as a result of the war, which is unfortunate," Rossini said.

Small business security

Ransomware attacks have not been limited to large organizations. Richard Clarke, chief insurance officer for Colonial Surety Co., said the concern for underwriters for small businesses is how well they know their customers and how those businesses authenticate potential access to their computers, networks and systems. Smaller businesses might be a little bit less equipped to deal with ransomware cyber extortion, he said.

After years of thinking they could stay under the radar as far as exposure to cybercrime goes, Clarke said small businesses are changing their attitudes, and demand for insurance and increased network security is rising.

"I think every business tries to put a cost-benefit factor on the premium versus their perception of the exposure," he said in an interview, adding that the premiums must be balanced against a business owner's perception of exposure.

"The aim is to get to the point where the small business owner will say: 'Yeah, I don't think that's such an unreasonable cost for that insurance protection.'"

This article was published by S&P Global Market Intelligence and not by S&P Global Ratings, which is a separately managed division of S&P Global.