Cyber: State of the Risk

Rising demand for cyber insurance – amid more frequent, more costly cybercrime incidents that have led some carriers to retreat from writing the coverage – is driving premiums sharply higher.

Ransomware attacks have affected critical infrastructure, schools, the food industry, and other entities in 2021, from the Colonial Pipeline to the Buffalo public school system to beef supplier JBS.

Ransomware attacks also hit insurers who write cyber coverage and ExaGrid – a backup-storage vendor that helps enterprises recover from ransomware attacks.

Once a diversifying secondary line and another policy endorsement, cyber insurance has become a primary part of any prudent corporation's risk-management and insurance-buying decisions.

Fast Facts

80% of survey respondents purchase some form of cyber insurance.*

Up from just 34% in 2011.

Stand-alone policies account for about **60% of premium**.

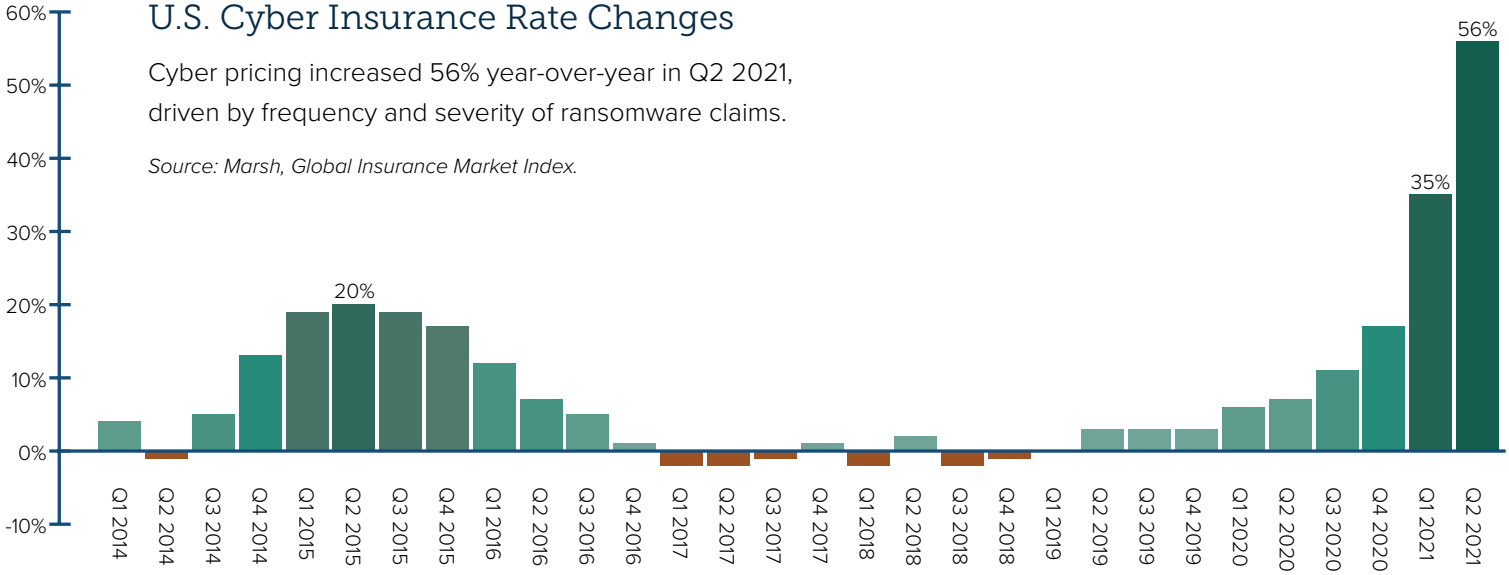
Although package policies account for about 95% of policies in force.

Learn More with Triple-I's
Facts + Stats: Identity Theft and Cybercrime

U.S. Cyber Insurance Rate Changes

Cyber pricing increased 56% year-over-year in Q2 2021, driven by frequency and severity of ransomware claims.

Source: Marsh, Global Insurance Market Index.



INSURANCE INFORMATION INSTITUTE

* Survey by data and analytics firm Advisen and global insurer Zurich

Cyber insurance purchases climb

A.M. Best calls the prospects for the cyber insurance market "grim" for several reasons:

- Rapid growth in exposure without adequate risk controls,
- Growing sophistication of cyber criminals, and
- The cascading effects of cyber risks and a lack of geographic or commercial boundaries.

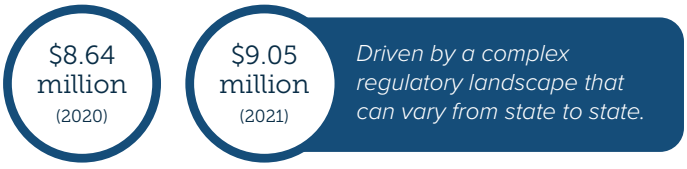
While A.M. Best says the industry is well capitalized, "individual insurers who venture into cyber risk without a thorough understanding of the market can find themselves in a vulnerable situation." Given the rapidly evolving cyber landscape, insurers are well advised to review risk controls, modeling, stress testing, and pricing, as well as their appetite for this peril.

"The cyber insurance industry is experiencing a perfect storm between widespread technology risk, increased regulations, increased criminal activity, and carriers pulling back coverage," according to Joshua Motta, co-founder and CEO of Coalition, a San Francisco-based cyber insurance and security company. "We've seen many carriers sublimit ransomware coverage, add coinsurance, or add exclusions."

A recent Willis Towers Watson study reported primary and excess cyber renewals averaging premium increases "well into the double digits." One factor helping to drive these increases, Willis writes, is the sudden shift toward remote work on potentially less-secure networks and hardware during the pandemic, which has made organizations more vulnerable to phishing and hacking.

The average cost* of a data breach:

Costs were highest in the United States:



* Report by IBM and the Ponemon Institute

Need for clarity

Despite the prevalence and severity of recent incidents, executives and other decision makers still need to better understand the risks, how to mitigate them, the available insurance products, and the limits to those coverages.

Many policyholders incorrectly still expect to be covered for cyber risk under their property and liability policies, according to Risk & Insurance, an affiliate of The Institutes and the Triple-I's sister organization. Such confusion can lead to unexpected coverage gaps for policyholders.

> "Cyber insurance is no longer a luxury item, even amid a hardening overall insurance market."
>
> – Advisen and Zurich survey

Of particular concern to insurers is silent – or "non-affirmative" – cyber risk, in which potential cyber-related events or losses are not expressly covered or excluded within traditional policies. In such cases, insurers can end up having to pay unexpected claims for which the policies weren't adequately priced.

Some in the national security world have compared U.S. cybersecurity preparedness today to its readiness for terrorist acts before 9/11, when terrorism risk was similarly "silent." Afterward, insurers began excluding terrorist acts from policies, and the U.S. government established the Terrorism Risk Insurance Act (TRIA) to stabilize the market.

The growing frequency and severity of cyber attacks could lead to a need for a similar federal backstop.

The Triple-I Blog

- Cyber Insurance's "Perfect Storm"
- "Silent" Echoes Of 9/11 in Today's Management of Cyber-Related Risks
- Brokers, Policyholders Need Greater Clarity on Cyber Coverage
- Cyber Risk Gets Real, Demands New Approaches