Cyber: State of the Risk

INSURANCE INFORMATION INSTITUTE
Affiliated with THE INSTITUTES

Remote work during the pandemic drove up costs associated with data breaches in 2021, according to a study by IBM and the Ponemon Institute.

An average data breach in 2021 cost $4.24 million, up from $3.86 million in 2020, the report says. However, where remote work was a factor in causing the breach, the cost increased by $1.07 million. At organizations with 81-100 percent of employees working remotely, the total average cost was $5.54 million.

Ransomware attacks alone rose by 105 percent globally in 2021, according to cybersecurity firm SonicWall. Ransomware attacks 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. They also hit insurers who write cyber coverage and ExaGrid – a backup-storage vendor that helps enterprises recover from ransomware attacks.

Direct-written premiums collected by the largest U.S. insurers increased by 92 percent year-over-year, and analysts say that mainly reflects higher rates, rather than insurers expanding the size of the claims they are willing to cover.

Fast Facts

10% increase
in average total cost of a breach, 2020-2021*

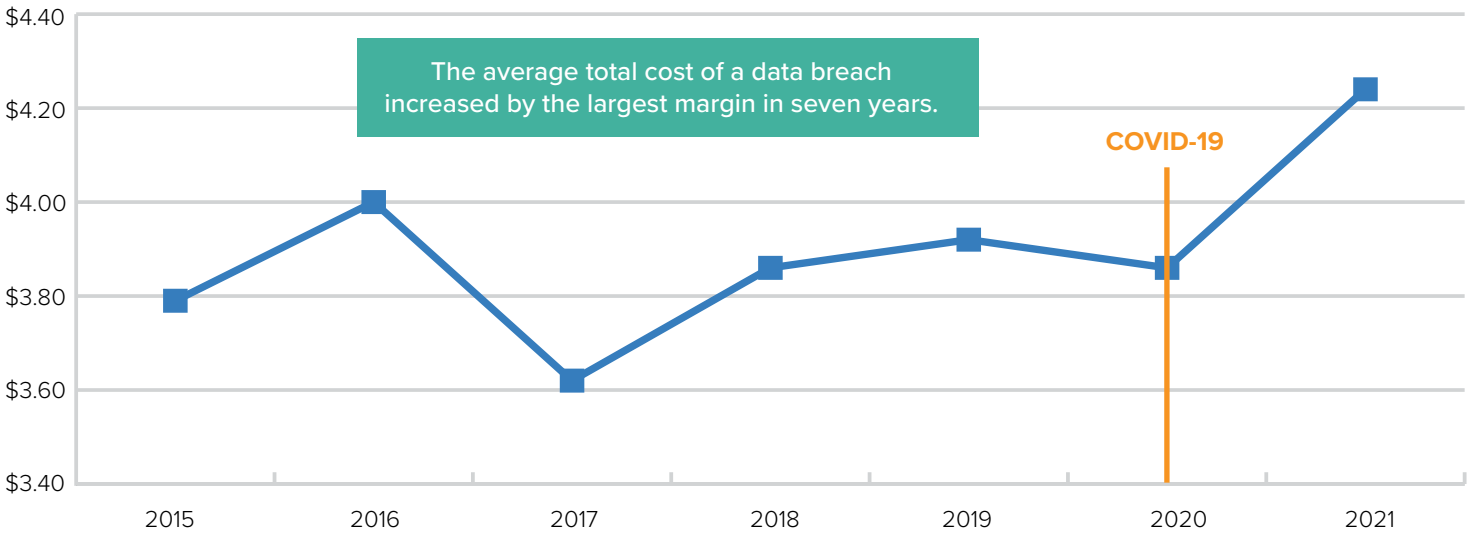
$1.07 million
cost difference where remote work was a factor in causing the breach*

11 consecutive years
healthcare had the highest industry cost of a breach*

Check Out Triple-I's Cyber Insurance Explainer Video

Average total cost of a data breach*

Measured in US $ millions



* Report by IBM and the Ponemon Institute

A "perfect storm"

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

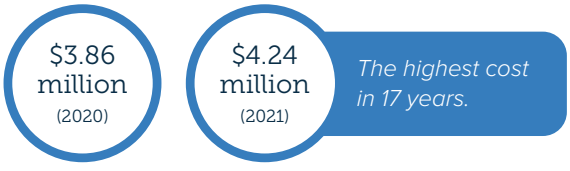
- Rapid growth in exposure without adequate risk controls,
- Growing sophistication of cyber criminals, and
- The cascading effects of cyber risks and a lack of geographic or commercial boundaries.

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.

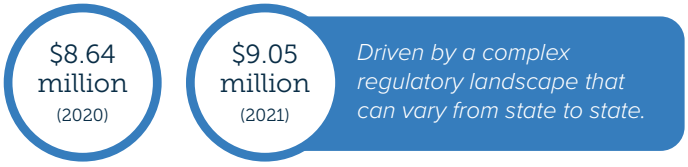
"The cyber insurance industry is experiencing a perfect storm between widespread technology risk, increased regulations, increased criminal activity, and carriers pulling back coverage," according to Joshua Motta, co-founder and CEO of Coalition, a San Francisco-based cyber insurance and security company. "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.

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

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.

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

- Cyberattacks Growing in Frequency, Severity, and Complexity
- Study Highlights Cost of Data Breaches in a Remote-Work World
- As Cybercriminals Act More Like Businesses, Insurers Must Think More Like Criminals
- Cyber Insurance's "Perfect Storm"
- "Silent" Echoes Of 9/11 in Today's Management of Cyber-Related Risks