BEST'S REVIEW®

ISSUES & ANSWERS: EVALUATING RISK IN THE EVOLVING CYBER MARKET

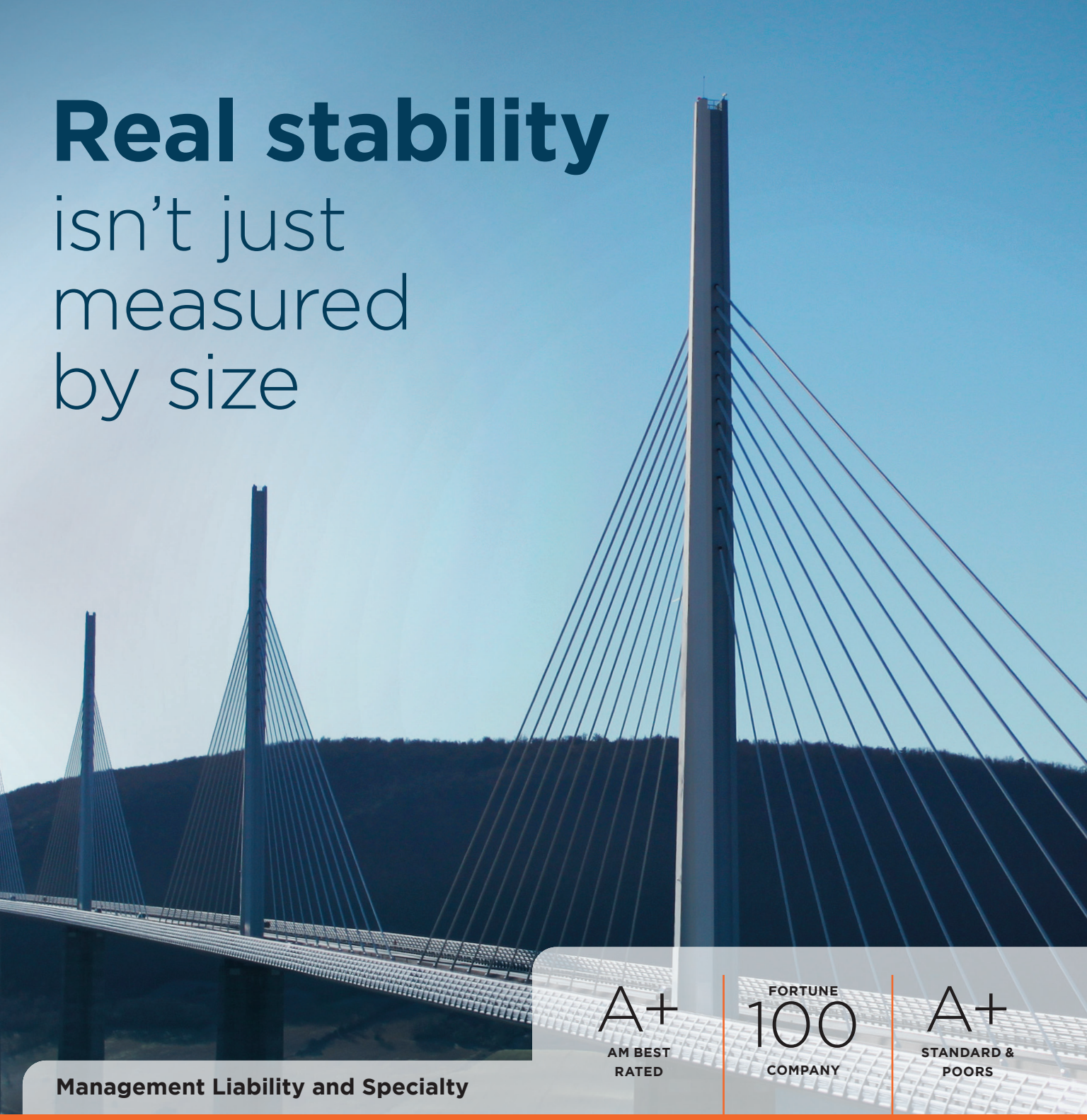
An industry expert discusses how cyber insurance can provide tools to help minimize the fallout from security breaches.

Interviewed Inside:

Tim Nunziata
Nationwide

View past Issues & Answers sections at
https://bestsreview.ambest.com/issuesanswersarchive.html

Real stability isn't just measured by size



A+
AM BEST RATED

FORTUNE 100
COMPANY

A+
STANDARD & POORS

Management Liability and Specialty

We are proud to be part of a company that's among the largest in our industry. But we take the greatest pride in the strong, stable relationships we've built with our partners through our commitment to service.

nationwide-mls.com

Nationwide®

A Day at the Breach

Tim Nunziata, VP and Head of Cyber Risk, Nationwide Management Liability and Specialty, said that when it comes to a cyber breach, there are a number of tools an insured can use to fight back. "They are available from the carrier to help improve the organization's risk profile, which is a good thing for everybody," he said. Following are excerpts from an interview.

Nationwide®

Tim Nunziata

VP and Head of Cyber Risk
Nationwide Management Liability and Specialty

"When it comes to a cyber breach, insureds need to know that it's not a matter of 'if' one will happen, but rather a matter of 'when' it will happen."

Visit the Issues & Answers section at *bestsreview.ambest.com* to watch an interview with Tim Nunziata.

How is underwriting evolving in the cyber insurance market?

We have been improving the underwriting process along the way. One of the biggest challenges is gathering consistent submission information —being able to evaluate risk on consistent and thorough information. Buying habits were lagging historically and not up to speed on the information gathering necessary to procure cyber insurance policies. There's also been a limited amount to claims activity historically in the space. That's now accelerating, and we're seeing and we're seeing increased loss trends.

How do you manage aggregation risk in this increasingly interconnected business world?

As the products have become more sophisticated, and our underwriting ability has become more thorough, we've been able to limit fallout through exclusionary language. Insureds are realizing they want the coverage to minimize some of that fallout. Historically, where they might want to provide some broad extensions for potential contingent losses, we are able to insulate those exposures and dedicate those limits to the intended insurance. Policy limits shouldn't be paying for losses elsewhere, so providing clarified language on what the intention of that coverage is important. It's threefold: identifying those exposures and minimizing our direct insurance of them; trying to underwrite to some of those direct interconnectivities; and ultimately using language to clarify the intent of the policy.

What resources and tools are out there for companies?

Internally, we have a risk evaluation system that allows us to evaluate not only the individual portfolio for risk that we might be underwriting, but allows us to evaluate the aggregation exposure across our portfolio, certain industries and identify areas of concern for systemic risk. It also allows us to model certain cyber incidents. Our model runs 10,000 potential scenarios against an insured's risk profile. That provides us with an exposure and severity score. While all these tools are in their infancy, they are rapidly maturing.

Why is pre-breach preparation so important?

Everybody thinks their system is buttoned up until it's too late. The cost associated with pre-breach resources is a drop in the bucket relative to the cost both reputationally and financially that would impact an organization when there is a breach. The bad actors are sophisticated and evolving. And the majority of time, the public is made aware when there is an incident. So it's about being prepared. When that cyber incident occurs, you need to be able to flip that switch, because the first 48 hours are critical. Based on penetration or exposures, insurers need to make sure that you have not only a familiarity with what the next couple of days or weeks may look like, there also needs to be a series of individuals and resources that are activated to streamline the restoration process. This includes legal services, forensics or public relations. There are a lot of moving pieces in that initial breach response and having all those ducks in a row is important. If you start to build that out or look to that up post-breach, by the time you know what's going on, it's going to be too late.