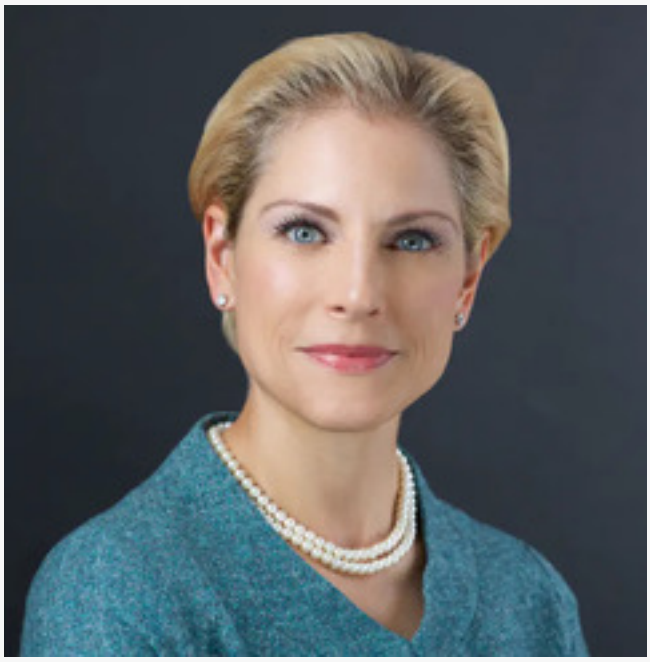
The New Rules for Successfully Underwriting Mid-Market Cybersecurity IT Risk -- Kirsten Bay, Cysurance

NEW YORK, UNITED STATES, October 18, 2023 /EINPresswire.com/ -- Managing risk in the mid-market sector has evolved into a complicated -- and often intractable -- challenge for senior leaders. Bad actors increasingly see companies in this segment as attractive targets because they often under-resource security initiatives. Small and medium-sized enterprises also tend to present a gateway to larger targets through supply-chain relationships, according to Kirsten Bay, CEO of Cysurance -- a next-generation risk mitigation company that insures, warrants and certifies security solutions deployed by enterprise end-users -- in a podcast interview for journalists.


Kirsten Bay, Cysurance

To address today's worsening threat landscape, mid-market organizations are exploring cyber insurance offerings. As they do, many are learning of the immense gaps that exist between current mid-market security efforts and the ability of the insurance industry to underwrite cyber risk.

> Today, organizations may pay as much as 150% more for premiums per million dollars in covered risk than they did a few short years ago."
> *Kirsten Bay, CEO of Cysurance*

"The cyber insurance market is challenging because there has been a significant reduction in available capital to write policies. As a result, it has not been unusual for organizations to see their cyber coverage drop from $10 million to $6 million. Adding insult to injury, premiums have risen dramatically. Today, organizations may pay as much as 150% more for premiums per million dollars in covered risk than they did a few short years ago. This means organizations are paying more for $6 million in coverage than they were for $10 million," she adds.

The primary reason for this dynamic lies in the inability of mid-market companies to effectively respond to threats. A recent McKinsey survey of 4,000 midsized companies suggests that threat volumes doubled from 2021 to 2022. Adversaries are growing in number and demonstrating higher levels of innovation over time. Nearly 80 percent of attackers -- and 40 percent of the malware used -- were new to cybersecurity staff.

It illustrates how far behind most players in the mid-market have fallen in the cyber arms race. According to McKinsey, there is a clear under-penetration of cybersecurity products and services, suggesting security budgets are underfunded, improperly deployed, or both. While this is bad news for companies in the segment, the trend is a source of extreme concern for insurance companies.

"Breaches -- especially ransom attacks, propagated predominantly by phishing -- are rising and causing significant losses. The ramifications of this, however, are often not fully understood by mid-market executives. From a cyber-insurance perspective, this phenomenon has led to disturbing trends on loss claim limits; instead of $100,000.00 claims being filed on million-dollar cyber policies, we see million-dollar claims."

The main consequence of companies' inability to limit losses is that the sector has generally become unviable to insure. It is a challenge exacerbated by the fact that too many leaders in the segment have come to view insurance policies as a substitute for establishing effective cyber security risk management protocols.

"Many organizations use the insurance policy application process as a way to benchmark their security controls. It is not a good practice. And it's not because the questions on insurance applications are necessarily wrong. The problem with the approach is that organizations end up focusing on things that have already happened when, in fact, most attacks are novel," says Bay.

A more constructive approach is to develop proactive rather than reactive strategies that are based on an intimate understanding of organizations' attack surfaces and the investments in solutions needed to address their specific threats, risks and consequences.

The National Institutes of Standards and Technology (NIST) cybersecurity frameworks, advises Bay, offers a systematic approach to improving the management of risks directly related to evolving cybersecurity realities. It also provides the basis for inter-organizational collaboration to identify and respond to zero-day attacks through real-time monitoring.

Establishing a sustained strategic focus on cybersecurity stimulates essential conversations between the executive suite and security practitioners. It elevates conversations about the talent, technology and processes that require investment to make organizations more resilient. Organizations that pursue this strategy significantly reduce their risk profile. Consequently, they become much more attractive for insurance companies to underwrite.

###

Editor’s Note: You can view the full interview with Kirsten Bay by visiting: https://www.cysuranceinstitute.com/insights/the-new-rules-for-successfully-underwritingnbspnbspmid-market-cybersecurity-it-risk-kirsten-bay-cysurance

Airrion Andrews
Cysurance
email us here