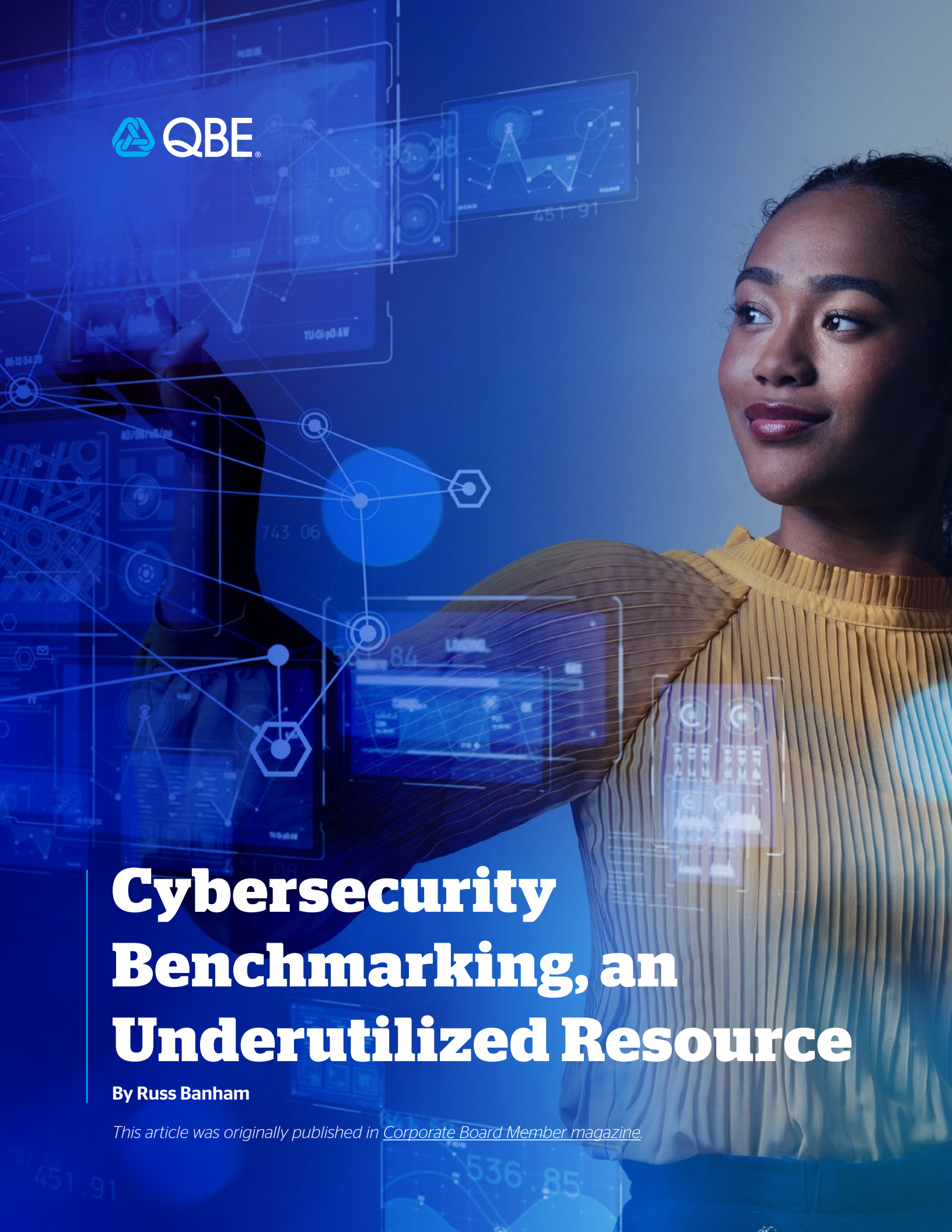

Cybersecurity Benchmarking, an Underutilized Resource

By Russ Banham

This article was originally published in Corporate Board Member magazine.

Boards struggling to evaluate cyber risk preparedness, recovery and response strategies are turning for advice to the last line of defense — insurance brokers and carriers.

Along with other risks like the economy, geopolitical tensions and climate change exposing corporate balance sheets to shocks, board members must now grapple with the growing regularity and financial costs of cyberattacks. With threat actors leveraging technological advances like Generative AI and automation to refine and increase the number of phishing scams, cyber risk is fast becoming corporate enemy number one.

That's the conclusion of a recent survey of more than 1,100 board members and C-suite executives. Asked to prioritize their top five business threats in 2024 and 2034, cyber risk came in third place in 2024 but rose to become the top risk in 2035. A key reason is ransomware attacks, which increased 84 percent year-over-year in 2023.

> ***"Here is this fantastic, underutilized resource for boards that also happens to be the last line of defense."***

Well aware of this growing menace, many board members entrusted to oversee the management of cybersecurity, risk mitigations and recovery plans reach out for advice to third party cybersecurity professionals. Few boards, however, have turned to the specialized expertise of insurance brokers and carriers, an omission that is now changing. The reason is clear: The insurance industry bears the brunt of catastrophic losses attributable to a major cyberattack. To provide this invaluable risk-bearing capacity, insurance carriers microscopically assess the potential for losses on a business-by-business basis.

"Boards want assurance that management has enough first-party and third-party insurance coverage to protect the balance sheet; not only can insurers provide this assurance, their underwriting assessments illuminate the specific cyber vulnerabilities of each organization and the adequacy of its cybersecurity investments," says Shamla Naidoo, Head of Cloud Strategy & Innovation at global cybersecurity leader Netskope and former Chief Information Security Officer (CISO) at IBM Global.

The experiences of many CISOs and other InfoSec leaders with their organization's insurance carriers substantiate this value. Prior to the sharp increase in ransomware attacks in the mid-2010s, CISOs annually filled out a simple one-page insurance application. Today, these forms, used by insurers for cyber liability underwriting and pricing, are dozens of pages long and packed with detailed and complex questions. From a risk benchmarking standpoint, no other industry has such comprehensive information on cyber risks. As Naidoo put it, "Here is this fantastic, underutilized resource for boards that also happens to be the last line of defense."

Boardroom Essentials

As a trained economist with a career spanning forty years, Naidoo is a technology industry veteran. After receiving her law degree from the University of Illinois Chicago School of Law, she successfully led cybersecurity strategy and risk management programs for several global companies. Having lived through some of the earliest instances of cyberattacks by nation-state actors, Naidoo has worked with intelligence communities to protect businesses and society from technology misuse.

Naidoo's deep cybersecurity expertise has drawn the attention of several boards: She is an independent board director today serving three publicly traded companies, including QBE North America, a large global insurer, Stonebridge Acquisition Corporation, a bridge for IPO-ready companies in Asian and EMEA regions to access the US markets, and WisdomTree, a global ETF (exchange-traded fund).

Few companies have sitting board members with such rarefied expertise. According to a September 2023 report by the Wall Street Journal, only 2.3 percent of board directors serving S&P 500 companies have any cybersecurity experience, impelling many boards to seek the advice of third-party security consultants. To guide board members in their Q&A sessions with these advisers, Naidoo coauthored the book, "The Cyber Savvy Boardroom: Essentials Explained," with another longtime cybersecurity expert and board director, Homaira Akbari. "Our goal was to give board directors a base understanding of cybersecurity to provide the same comfort they feel with oversight of other business threats," she says.

The book, for example, offers a common-sense approach to questions that determine whether management is taking necessary security measures at an appropriate cost to protect the balance sheet. An entire section of the book is devoted to cyber insurance, citing the financial protection provided for data breaches, network failures and cyber extortion.

"The board needs to ask questions to confirm the insurance policy is comprehensive and well-designed," Naidoo says. "Some but not all cyber insurance policies cover incident response expenses absorbing legal fees, the replacement of damaged data and systems, and lost business income while systems are down and inaccessible."

Following the July 2023 adoption and implementation of the Securities and Exchange Commission's Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure regulation, such questions have become crucial for board members to ask. The regulation requires publicly traded companies to report a material cyber incident in four days and also provide detailed information on their cyber risk management, strategy and governance. "The adequacy of a company's insurance policies to transfer catastrophic cyber risks would likely be considered 'material information' to shareholders," she explains.

> ***"The adequacy of a company's insurance policies to transfer catastrophic cyber risks would likely be considered 'material information' to shareholders,"***

With advanced technologies like GenAI and automation now in the hands of threat actors, boards must ensure the investments in cybersecurity promote the growth and success of the business, says Naidoo. "At the same time, given their fiduciary obligations to shareholders, board members need assurance that their actions or inactions don't contribute to their own liability."

Such breaches of duty include a failure to comply with SEC regulations or the lack of effective governance, each potentially resulting in personal liability for board members. Given this dire possibility, an insurer with expertise in underwriting both cyber insurance and directors and officers' liability (D&O) insurance can provide board members with "comprehensive risk protection," says Serene Davis, Global Head of Cyber at QBE.

The large global insurer is a provider of both cyber and D&O insurance policies. "We can help board members questioning the state of their organization's cyber risk readiness and resiliency," Davis says. "We've just begun benchmarking our book of cyber insurance policyholders to assess how businesses on an anonymous basis in different industry sectors stack up against their peers on a cyber preparedness, response and recovery basis."

The analyses may become invaluable for board directors seeking greater assurance about cyber risk management in compliance with the SEC cybersecurity regulation, says Davis. Naidoo concurs that the opportunity for boards to access benchmarking criteria on peers is a valuable resource, "encouraging them to ask questions on why this is the case to the CISO and management," she explains.

Time is of the essence for all boards to become more "cyber savvy," to borrow from the title of Naidoo and Akbari's book. Last year, the average cost of a single data breach globally increased 15 percent year-over-year to $4.45 million, on the way towards cyber threats becoming the number one business risk in 2034.