CONTRIBUTOR CONTENT

Dave Chatterjee Drops the Cybersecurity Jargon, Encouraging Proactiveness Rather than Reactiveness

Tyler Shepherd Contributor
Published 1:44 p.m. ET April 8, 2024

Cybersecurity, a term often used lightly, seldom understood, and frequently understated, has entered the public sector without warning, confusing many business owners and inexperienced individuals. While adequate mainstream implementation of cybersecurity still has a long way to go, with only 40% of business leaders believing cybersecurity threats will 'highly affect' the organization's performance, the impact of security breaches can't be ignored, calling for immediate action, education, and widespread awareness.

According to recent statistics published by Forbes, there were 2,365 cyberattacks in 2023, affecting over 343 million victims. Last year also saw a 72% increase in data breaches since 2021. The most common malware method was executed via email (35% of all breaches), and a staggering 94% of companies have reported email security issues. If successful, a cyberattack costs an organization $4.45 million on average, posing a significant threat to companies worldwide, specifically small and medium ones.

While cyberattacks are undeniably one of the most prominent threats modern-day companies face, many business leaders undermine the far-reaching consequences of insufficient security systems. Dr. Dave Chatterjee, a Cybersecurity and Technology Expert, an Associate Professor at the University of Georgia, a visiting Professor at Duke University, and a fervent advocate of competent security measures, has devoted his career to spreading awareness about the threats of cyberattacks and data breaches, empowering businesses to take an educated proactive stance.

Dr. Dave

Cybersecurity, or the practice of protecting internet-connected systems from cyber threats, is often mistakenly considered a strictly technological issue, deterring those with little to no tech background from taking action. Industry-specific jargon and scientific terminology turn cybersecurity into a far-flung concept rather than a tangible aspect of day-to-day life, and grasping the complexities of cybersecurity is unviable for most company leaders. That's why senior leadership's attention to this critical challenge is often inadequate.

"I take a holistic approach to cybersecurity readiness," says Dr. Dave. "By holistic, I mean taking every aspect of cybersecurity into account—the technical side, the non-technical side, and the leadership side. I believe that in the long run, mainstream operations at an ample level of cybersecurity proficiency can only be possible if the organizational culture becomes more cyber-savvy."

The renowned Professor and thought leader curated an empirically validated framework designed to enable businesses to tackle universal cyber-related risks. The framework, called Commitment, Preparedness, Discipline (CPD), is a meticulously crafted guide for organizations on how to approach cybersecurity from a long-term strategy perspective rather than the 'checking the boxes' angle. The framework came to life after Dr. Dave performed qualitative analysis, identifying 17 success factors and attributing them to the three dimensions: Commitment, Preparedness, and Discipline.

For instance, Dr. Dave recognized Hands-On Top Management as a crucial success factor, ascribing it to the Commitment basket. "From my experience, I have learned that organizations where senior leadership employees make an active commitment to security have an attractive edge in terms of readiness. They're not only talking about cybersecurity but walking the talk, leading by example," adds Dr. Dave. Backed by research and experience, the CPD framework is a trusted method within the industry.

"It's relatively easy to check off the compliance boxes, however, substantive implementation is key to success," says Dr. Dave. The issue lies in educating senior leadership and making them realize the essential value of cybersecurity, even in companies that belong to drastically different sectors. "Even if cybersecurity is not the focus of your business, recognizing and developing this strategic capability is essential to long-term competitive success. To achieve a safer future, more leaders should strive to make cybersecurity a core competency. That's easier said than done. My framework sensitizes management, shifting leaders' mindsets from considering cybersecurity merely as a necessity to thinking of it as a strategic opportunity. If customers believe a company takes its cybersecurity responsibility seriously, they will be more trusting and keener to share data and use its services."

Cybersecurity, just like any tech-oriented industry, is constantly evolving, with new regulations and developments introduced daily. That's why staying informed and on top of the news is crucial in maintaining a cyber-safe organization. Through the Cybersecurity Readiness Podcast, Dr. Dave has a constant inflow of relevant expertise coming his way. Frequent jargon-free conversations with subject matter experts equip him with an encompassing spectrum of technological leadership knowledge, evoking thought-provoking ideas on enhancing cybersecurity at an individual, organizational, and national level.

The Cybersecurity Readiness Podcast Logo

Further fueling his expertise, Dr. Dave authored *Cybersecurity Readiness: A Holistic and High-Performance Approach*, a book exposing the challenges organizations face regularly and offering strategic insights on building stable cybersecurity programs. "The purpose of the book is to instill a holistic approach to cybersecurity readiness in the masses," adds Dr. Dave. Realizing that cybersecurity is everyone's business, the book is devoid of complicated tech terminology and industry-specific jargon, making extensive and invaluable knowledge accessible to non-tech individuals.

Cybersecurity Readiness Book Cover

The rising digitization in recent years has highlighted the importance of competent security systems even more. Systems are now interconnected, businesses entwined, and people bound, all due to the power of the Internet. That integration, although resulting in a more scalable and efficient dynamic, increases cyberattack surfaces. If perpetrators breach one system, almost like a domino effect, all systems connected are at risk.

In the face of modern developments and repercussions associated with data breaches, far too many organizations still take the reactive rather than proactive approach. While large corporations and industry giants can weather the economic struggles of cyberattacks, small and medium companies are the most susceptible to experiencing the disastrous impact of data breaches.

'How do I create an organizational culture where everybody recognizes their role transcends main tasks and extends to being security conscious?' is a question Dr. Dave believes all leaders should frequently ask themselves. Through education, a holistic approach, and a steadfast commitment to fostering a high-performance security culture, organizations will be able to maintain a steady upward trajectory, etching cybersecurity into the company's DNA.

"Cybersecurity performance is not something we should allow to fluctuate. The repercussions are too drastic, and the risks are too high. We saw the implications of reacting too slowly to the COVID-19 Pandemic. Far too many leaders take a reactive approach to cybersecurity, and we could see an equally catastrophic breakdown in society as we did then if we do not prepare ourselves," adds Dr. Dave. "For me, cybersecurity is more than just an extra cost of running a business; it's a necessity and the only way to ensure a safe future."

Members of the editorial and news staff of the USA TODAY Network were not involved in the creation of this content.

More from Contributor Content

From the Big Box Boom to the Online Shopping Explosion: Retail Trends in E-commerce Furniture

Eyal Baumel: Insights from working with top creators MrBeast and Lika Nastya