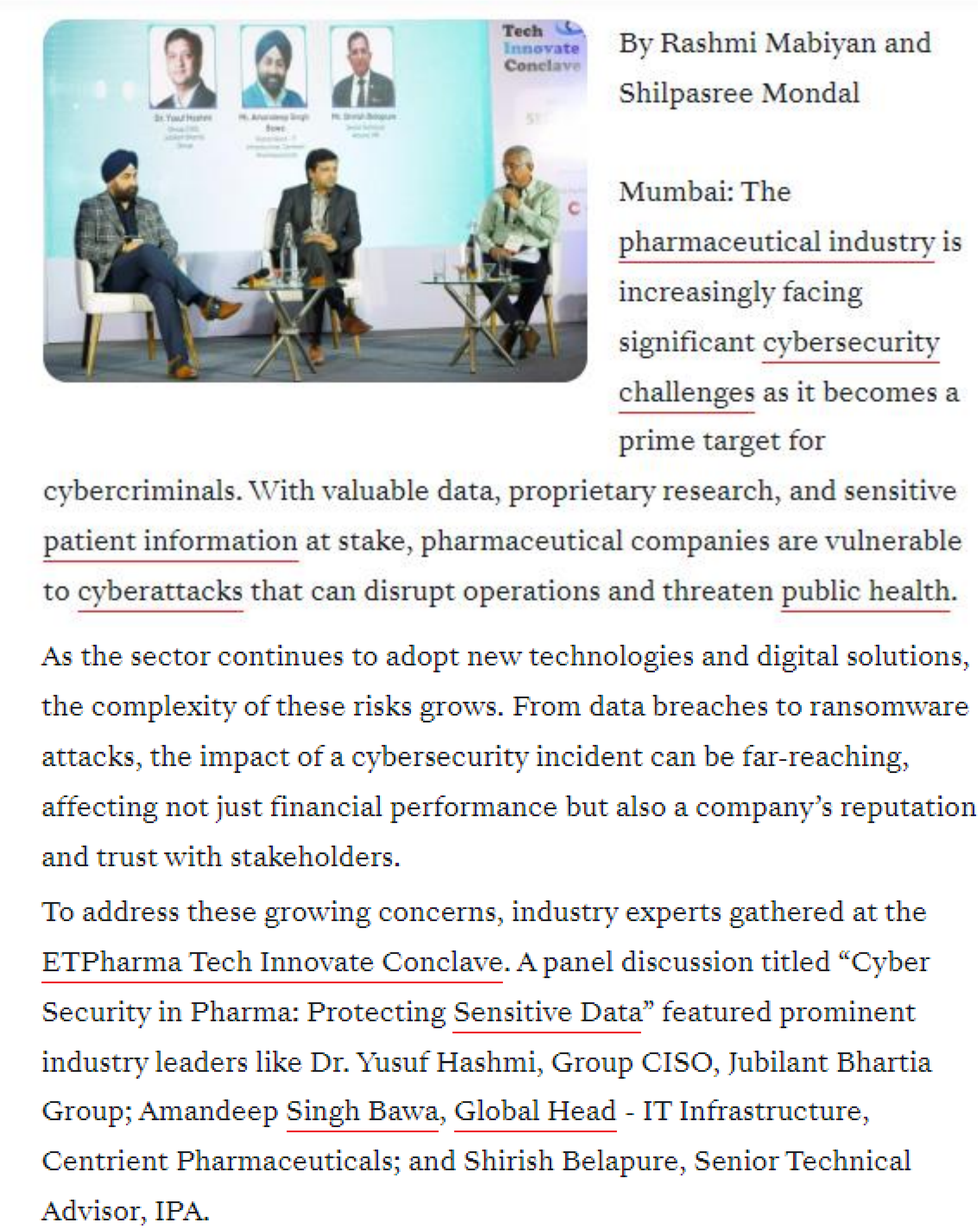
ETPharma Tech Innovate Conclave: Pharma sector faces rising cyber risks, say experts

As the sector continues to adopt new technologies and digital solutions, the complexity of these risks grows. From data breaches to ransomware attacks, the impact of a cybersecurity incident can be far-reaching, affecting not just financial performance but also a company's reputation and trust with stakeholders.

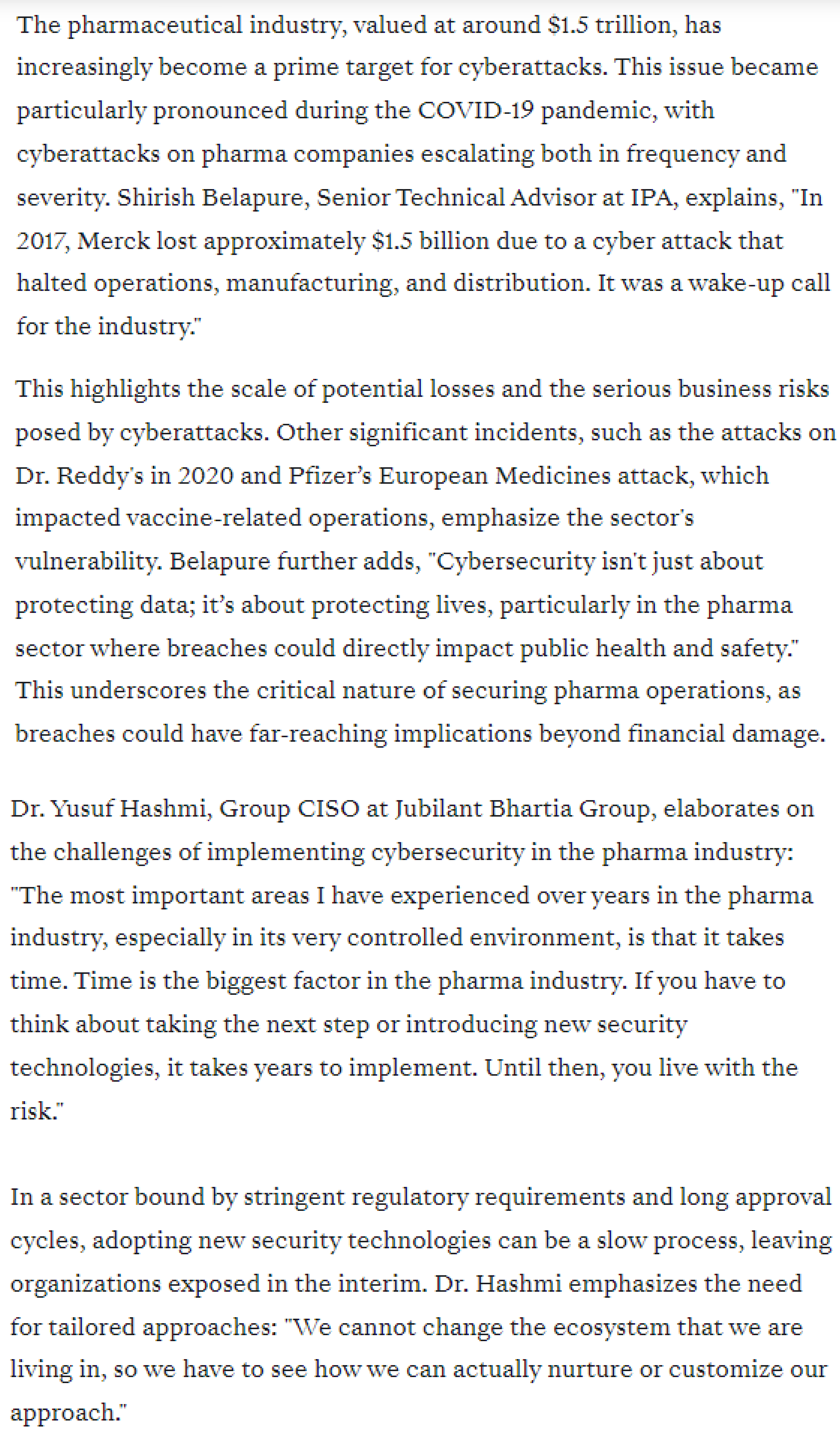


By Rashmi Mabiyan and Shilpasree Mondal

Mumbai: The pharmaceutical industry is increasingly facing significant cybersecurity challenges as it becomes a prime target for cybercriminals. With valuable data, proprietary research, and sensitive patient information at stake, pharmaceutical companies are vulnerable to cyberattacks that can disrupt operations and threaten public health.

As the sector continues to adopt new technologies and digital solutions, the complexity of these risks grows. From data breaches to ransomware attacks, the impact of a cybersecurity incident can be far-reaching, affecting not just financial performance but also a company's reputation and trust with stakeholders.

To address these growing concerns, industry experts gathered at the ETPharma Tech Innovate Conclave. A panel discussion titled "Cyber Security in Pharma: Protecting Sensitive Data" featured prominent industry leaders like Dr. Yusuf Hashmi, Group CISO, Jubilant Bhartia Group; Amandeep Singh Bawa, Global Head - IT Infrastructure, Centrient Pharmaceuticals; and Shirish Belapure, Senior Technical Advisor, IPA.

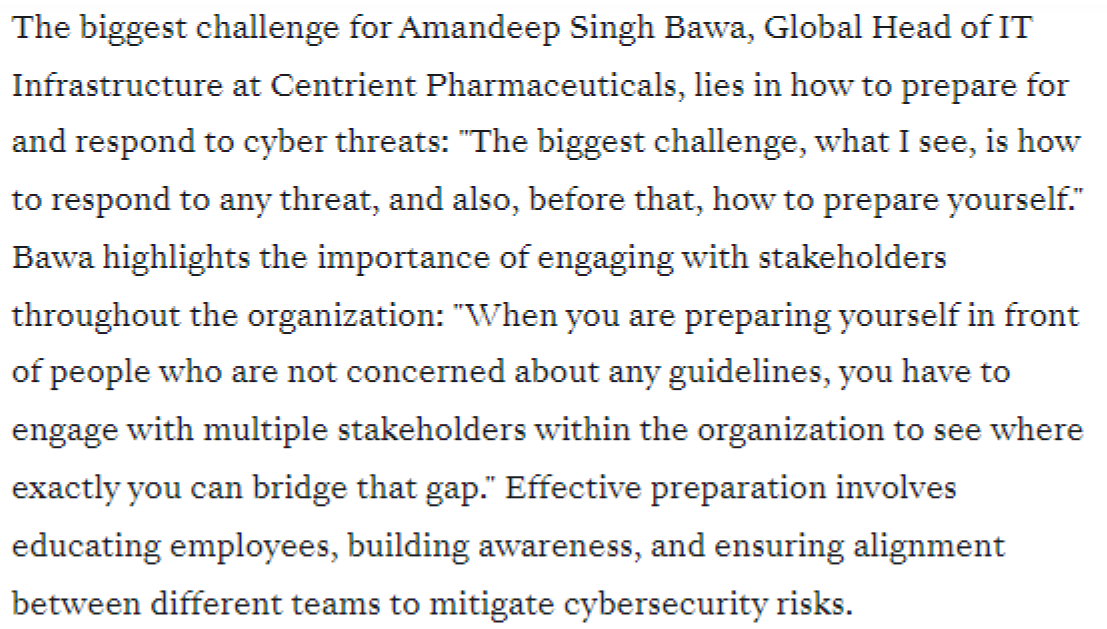


The pharmaceutical industry, valued at around $1.5 trillion, has increasingly become a prime target for cyberattacks. This issue became particularly pronounced during the COVID-19 pandemic, with cyberattacks on pharma companies escalating both in frequency and severity. Shirish Belapure, Senior Technical Advisor at IPA, explains, "In 2017, Merck lost approximately $1.5 billion due to a cyber attack that halted operations, manufacturing, and distribution. It was a wake-up call for the industry."

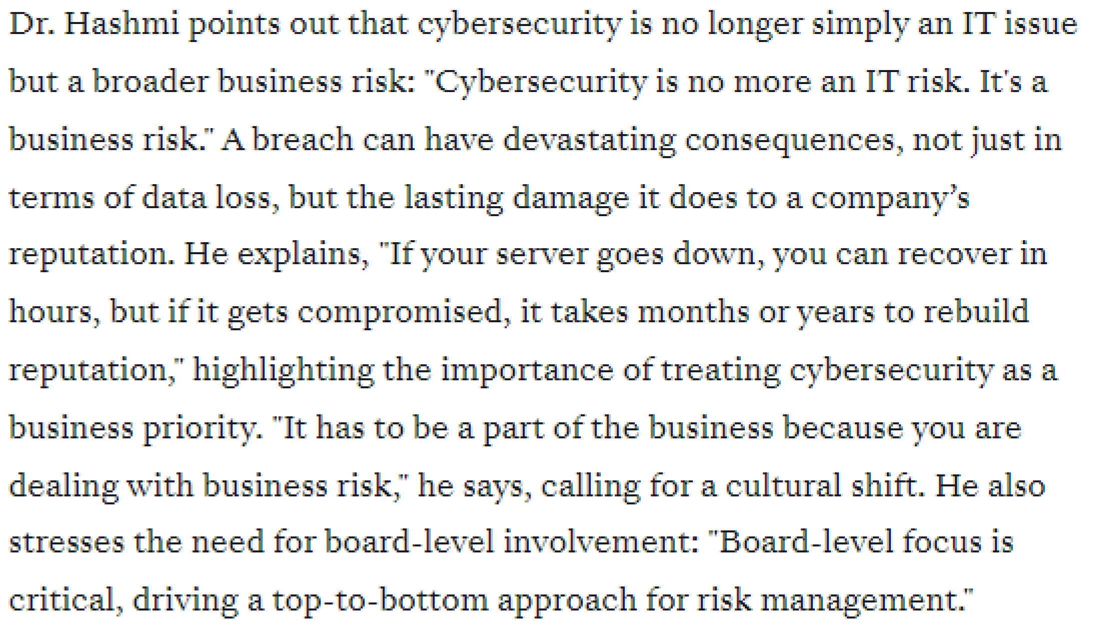
This highlights the scale of potential losses and the serious business risks posed by cyberattacks. Other significant incidents, such as the attacks on Dr. Reddy's in 2020 and Pfizer's European Medicines attack, which impacted vaccine-related operations, emphasize the sector's vulnerability. Belapure further adds, "Cybersecurity isn't just about protecting data; it's about protecting lives, particularly in the pharma sector where breaches could directly impact public health and safety." This underscores the critical nature of securing pharma operations, as breaches could have far-reaching implications beyond financial damage.

Dr. Yusuf Hashmi, Group CISO at Jubilant Bhartia Group, elaborates on the challenges of implementing cybersecurity in the pharma industry: "The most important areas I have experienced over years in the pharma industry, especially in its very controlled environment, is that it takes time. Time is the biggest factor in the pharma industry. If you have to think about taking the next step or introducing new security technologies, it takes years to implement. Until then, you live with the risk."

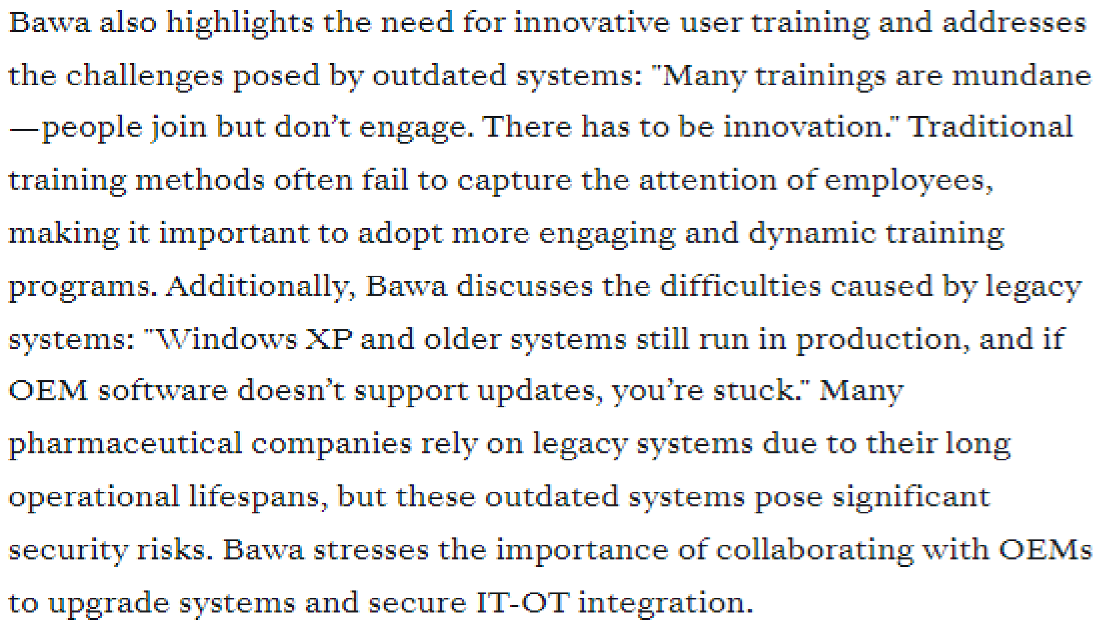
In a sector bound by stringent regulatory requirements and long approval cycles, adopting new security technologies can be a slow process, leaving organizations exposed in the interim. Dr. Hashmi emphasizes the need for tailored approaches: "We cannot change the ecosystem that we are living in, so we have to see how we can actually nurture or customize our approach."



The biggest challenge for Amandeep Singh Bawa, Global Head of IT Infrastructure at Centrient Pharmaceuticals, lies in how to prepare for and respond to cyber threats: "The biggest challenge, what I see, is how to respond to any threat, and also, before that, how to prepare yourself." Bawa highlights the importance of engaging with stakeholders throughout the organization: "When you are preparing yourself in front of people who are not concerned about any guidelines, you have to engage with multiple stakeholders within the organization to see where exactly you can bridge that gap." Effective preparation involves educating employees, building awareness, and ensuring alignment between different teams to mitigate cybersecurity risks.



Dr. Hashmi points out that cybersecurity is no longer simply an IT issue but a broader business risk: "Cybersecurity is no more an IT risk. It's a business risk." A breach can have devastating consequences, not just in terms of data loss, but the lasting damage it does to a company's reputation. He explains, "If your server goes down, you can recover in hours, but if it gets compromised, it takes months or years to rebuild reputation," highlighting the importance of treating cybersecurity as a business priority. "It has to be a part of the business because you are dealing with business risk," he says, calling for a cultural shift. He also stresses the need for board-level involvement: "Board-level focus is critical, driving a top-to-bottom approach for risk management."



Bawa also highlights the need for innovative user training and addresses the challenges posed by outdated systems: "Many trainings are mundane—people join but don't engage. There has to be innovation." Traditional training methods often fail to capture the attention of employees, making it important to adopt more engaging and dynamic training programs. Additionally, Bawa discusses the difficulties caused by legacy systems: "Windows XP and older systems still run in production, and if OEM software doesn't support updates, you're stuck." Many pharmaceutical companies rely on legacy systems due to their long operational lifespans, but these outdated systems pose significant security risks. Bawa stresses the importance of collaborating with OEMs to upgrade systems and secure IT-OT integration.

In the regulated environment of the pharma industry, implementing new technologies can be particularly complex. Dr. Hashmi explains, "Even adding an agent to a machine takes months due to rigorous validation and quality checks." Every change, no matter how small, needs to go through strict validation to ensure compliance with regulatory standards. He emphasizes the critical role of collaboration between IT, quality, and validation teams to ensure all security measures are in place before introducing new systems or technologies: "The IT, quality, and validation teams play a major role, ensuring all controls and assurances are in place before introducing anything new."

In global pharma operations, Amandeep Singh Bawa highlights the structured approach to managing changes: "We identify global and local changes and involve multiple stakeholders from different countries, each with their own norms, before making a decision. Quality plays a very strong role, maintaining close checks on what we do and its potential impact." This reflects the need for a detailed, organized process when making changes, as every decision can have far-reaching consequences. He adds, "IT has a nature to move quickly to adapt to market needs and respond to threats, but we are reminded to follow procedures that ensure product safety and connect to lives." Regulatory and quality checks must always remain a priority, even as the industry moves quickly to respond to new threats.

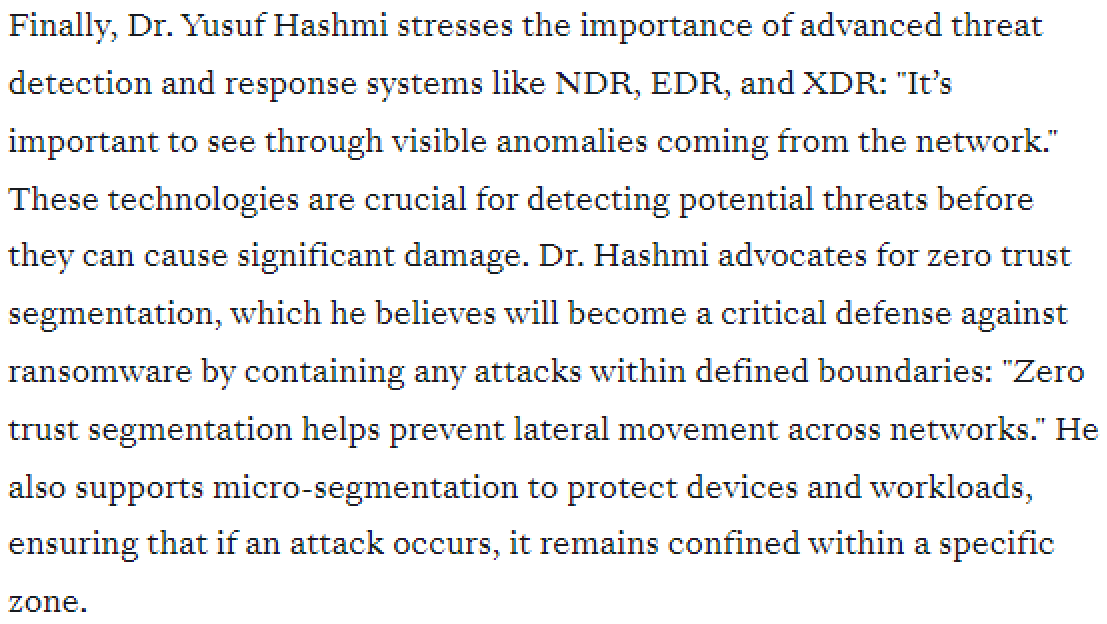
The threat of ransomware remains a major concern for pharma companies, and Dr. Hashmi explains the dire financial consequences: "The average recovery cost for ransomware in the pharma industry is $7.3 million, far higher than the $4.8 million average across industries." The financial and operational costs of a ransomware attack can be staggering. Dr. Hashmi emphasizes that mitigating ransomware risk requires a comprehensive approach: "Mitigating ransomware risk is not a one-day job. It requires 30 to 35 controls to protect the organization."

A multi-layered defense strategy is essential, including a combination of prevention, detection, and response mechanisms. He stresses that effective risk management must address three factors: probability, impact, and velocity. "Strategies must be tailored to each dimension to ensure effective mitigation." He highlights the importance of network visibility: "If your assets are not visible, you're more likely to face a ransomware attack."

Active Directory and VPNs are key areas of vulnerability, according to Dr. Hashmi: "Active Directory is the weakest link and can reduce ransomware risk by 70-80% if addressed effectively." Ensuring that these systems are secured can significantly lower the chances of a successful attack. A holistic approach is required to secure every aspect of an organization's infrastructure, from identity and devices to applications and networks.

Bawa further emphasizes the need for comprehensive visibility in all areas of the environment: "You have to have more visibility into your environment, not only about the data, but also about the hardware, the software, the tools, what you're using, how they are connecting to your environment, and how they are impacting your environment." This visibility is essential to building a strong defense. Bawa categorizes cybersecurity into two key areas: defense and response.

For defense, strong visibility, automation, identity and access management, zero trust, and segmentation play critical roles in protecting against cyber threats. He also highlights the risk posed by "zombie IDs," citing an example where "a stolen ID allowed someone to siphon out six crore rupees." Addressing such issues is critical to preventing insider threats and ensuring organizational security.



Finally, Dr. Yusuf Hashmi stresses the importance of advanced threat detection and response systems like NDR, EDR, and XDR: "It’s important to see through visible anomalies coming from the network." These technologies are crucial for detecting potential threats before they can cause significant damage. Dr. Hashmi advocates for zero trust segmentation, which he believes will become a critical defense against ransomware by containing any attacks within defined boundaries: "Zero trust segmentation helps prevent lateral movement across networks." He also supports micro-segmentation to protect devices and workloads, ensuring that if an attack occurs, it remains confined within a specific zone.

News Source:

https://pharma.economictimes.indiatimes.com/news/pharma-industry/etpharma-tech-innovate-conclave-pharma-sector-faces-rising-cyber-risks-say-experts/115973580?utm_source=whatsapp_web&utm_medium=social&utm_campaign=socialsharebuttons