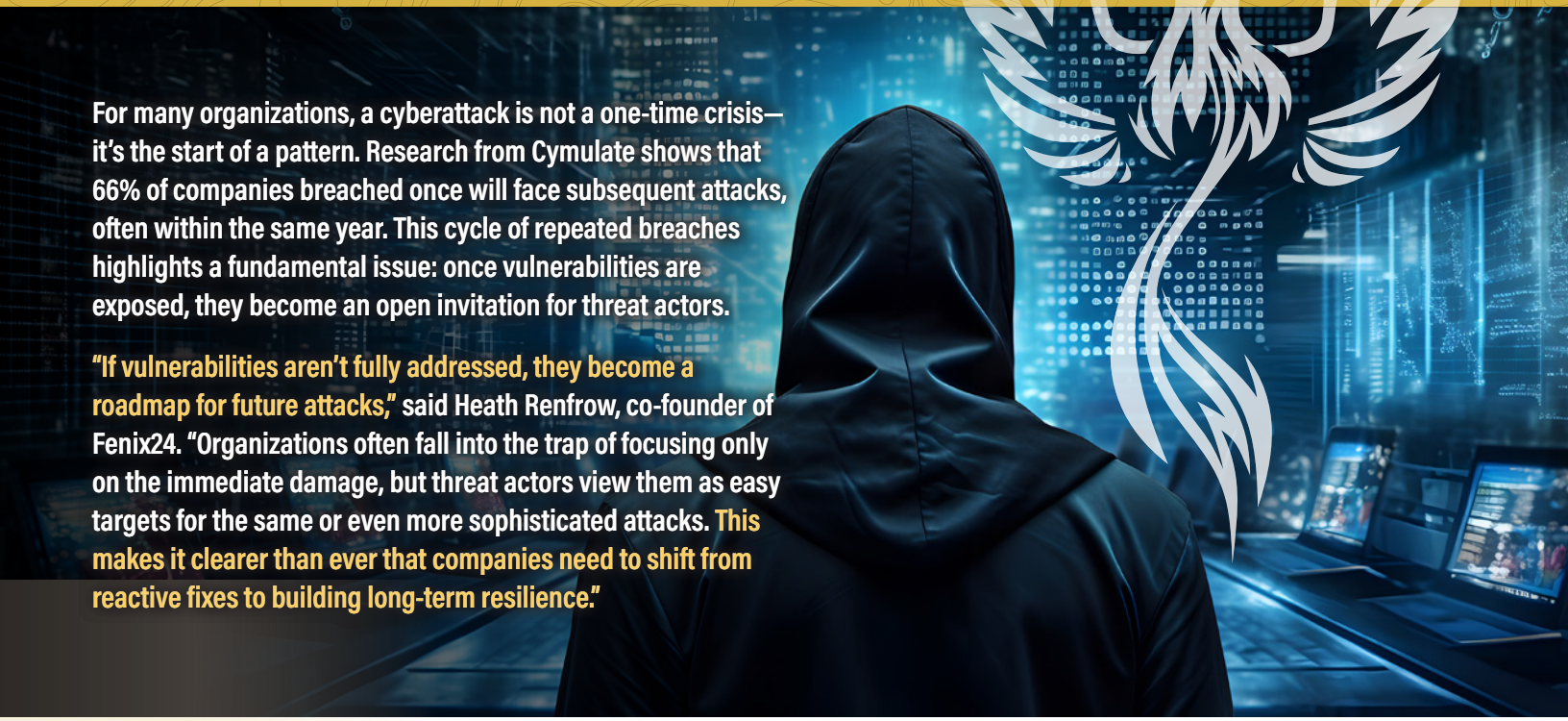
ONE BREACH IS NEVER THE END:

The Reality of Resilience, Recovery, and Repeat Cyberattacks



For many organizations, a cyberattack is not a one-time crisis—it's the start of a pattern. Research from Cymulate shows that 66% of companies breached once will face subsequent attacks, often within the same year. This cycle of repeated breaches highlights a fundamental issue: once vulnerabilities are exposed, they become an open invitation for threat actors.

"If vulnerabilities aren't fully addressed, they become a roadmap for future attacks," said Heath Renfrow, co-founder of Fenix24. "Organizations often fall into the trap of focusing only on the immediate damage, but threat actors view them as easy targets for the same or even more sophisticated attacks. This makes it clearer than ever that companies need to shift from reactive fixes to building long-term resilience."

How to Minimize the Risk of Repeated Breaches

To effectively reduce the risk of future attacks, organizations should prioritize a strategic overhaul of their security approach, including:

- Strengthen cybersecurity expertise at the executive level. Assign dedicated security officers, such as CISOs, and bring in external consultants if needed.
- Implement a systematic approach to applying patches and updates. Ensure that every known vulnerability is addressed quickly.
- Embrace a Zero Trust security model that limits internal access and requires verification for each request. This helps minimize the damage from insider threats and restricts lateral movement during an attack.
- Don't just focus on patching after a breach. Conduct a full security review to realign your company's approach to potential future attacks and consider a complete reset of your cybersecurity posture if necessary.

Resistance is important, but it's no longer enough. The ability to recover quickly after an attack is what defines true cyber resilience. Organizations that prioritize both resistance and recovery will minimize disruption and maintain business continuity.

Is your business prepared to recover when the inevitable happens? For more information on preventing repeated hacks or to schedule a consultation, contact Fenix24 at:
1.855.FENIX24, option2 rapidresponse@fenix24.com

FENIX24®
A CONVERSANT GROUP COMPANY