The current moment is one of transition. As organizations have increased their reliance on workplace flexibility and cloud computing, the role of cybersecurity leaders has transformed. The challenges of data protection, privacy, and compliance are more pressing than ever, and the threats from cyber attackers have evolved.

The rise of ransomware is a stark example. "Ransomware as a service" is behind the meteoric rise of this crime. Maturing cybercrime supply chains are enabling attackers to work harder to gain access to multiple targets with greater sophistication. The cost of a ransomware attack is now much higher, with more than half their data at risk. The severity of attack is growing too: ransomware attacks in 2021 were three times more severe than in 2020, and the average cost of a ransomware attack has increased by 87% since 2020.

In interviews, CISOs credit this proactive approach to their cyber hygiene to prevent the most common lines of breach. They report that they are more vigilant about their security model and guide future investments and risk management.

What security leaders can do:

1. Learn more about their most vulnerable digital feature. This could be their top priority. Our data and research support this finding.

2. Utilize multifactor authentication (MFA) and patching are still factors in the next two years.

3. Elevate cybersecurity into a strategic business function. This is the cornerstone of security, but a perimeter-based approach is no longer enough.

4. Enable multifactor authentication protection. This is crucial for securing the organization across multiple platforms.

5. Hire cloud experts. The cloud multiverse is becoming more critical.

6. Invest in training and knowledge. Knowledge is power in today's security threat landscape.

Elevate cybersecurity into a strategic business function and understand the fundamentals of security. This requires a focus on identity and access policies, minimizing the opportunity for attack, and making it harder for attackers to gain access. While mitigating the risk and minimizing the impact of attack, security leaders must embrace vulnerability as a feature of the hybrid work environment and seek ways to optimize for resilience rather than protection. In interviews, respondents who indicated maturity in their Zero Trust security posture—83% compared to 35% in 2020—showed a significant reduction in concern across nearly all security features. This finding is a noteworthy one given the consensus that cyber threats are a top concern among CISOs.

The data and research support this optimism. The cost of a data breach has declined in the past two years, with fewer respondents seeing networks as a significant security concern. Only IoT is expected to be as vulnerable as it is today; all other security features have improved. Furthermore, nine in ten security leaders who reported feeling vulnerable to cyber attacks in 2020 feel more secure today, with 61% of those who feel extremely vulnerable to attack now reporting a mature security posture (83%) and with viewing security more optimistically.

In summary, the role of security leaders is evolving, and they must adapt to the changing threat landscape. The rise of ransomware, the increasing reliance on cloud computing, and the shift to hybrid work are just a few of the challenges that demand a more proactive approach. Security leaders must elevate cybersecurity into a strategic business function, invest in training and knowledge, and embrace vulnerability as a feature of the hybrid work environment. Only then can they ensure that their organizations are resilient in the face of attacks.