Why Zero Trust Is a Strategic Imperative for Corporate Boards

Despite massive cybersecurity investments, breaches continue happening. Geopolitical instability and economic uncertainty are fueling a rise in cyber threats, while criminals use ransomware to extort money from victims. Legacy security architectures that rely on firewalls and VPNs can't keep up with the shift to mobile, cloud computing, and hybrid work patterns. Leading chief information officers are now adopting modern zero-trust architectures to minimize security risks while reducing network complexity and costs.

TRENDS & EMERGING ISSUES

Artificial intelligence is changing the threat and risk landscape, serving as a force multiplier for attackers. AI allows criminals to attack IT networks faster and more effectively by identifying specific vulnerabilities and creating attacks to exploit them. It simplifies the process of creating phishing emails that mimic the style of official communications and fake websites to steal user credentials.

However, AI delivers substantial benefits to defenders too. When paired with a modern architecture, it can detect the earliest signs of attacks and predict what attackers will do next, ensuring activity can be stopped before it causes damage.

CASE STUDY

Many organizations are stuck in a decades-old security model, relying on firewalls and VPNs that attackers can easily bypass with stolen credentials. Implementing a zero-trust architecture could make 90 percent of cyberattacks on companies disappear.

For example, a global electrical equipment manufacturer with 90,000 employees replaced legacy VPNs and firewalls with zero-trust connectivity and AI protections from Zscaler, as their old security architecture was incompatible with the company's cloud-first strategy. The phased deployment involved first protecting employee internet access and later protecting access to applications.

IMPACT

From day one, the result has been a more secure, reliable, and regulated user experience for employees and third parties. The company leverages AI for threat detection, data-loss prevention, visibility into the use of public AI applications, and segmentation to limit damage from any successful attack. The company reported four million threats blocked in one month. The new architecture also has fewer devices exposed to the internet—a reduced attack surface—giving attackers far fewer opportunities to compromise the network.

HOW TO MITIGATE RISKS

Reducing an organization's attack surface is a priority for cyber risk mitigation. Cybercriminals frequently target VPNs and firewalls as part of ransomware attacks because they are directly accessible from the internet and frequently contain unpatched vulnerabilities. Large companies typically have hundreds or thousands of these devices, which can be costly to procure and maintain. Zero trust reduces both the cost and complexity of IT networks while improving security and user experience.

QUESTION FOR YOUR NEXT BOARD MEETING

What is our timeline and strategy for transitioning to a zero-trust architecture that is aligned with our organization's business objectives and risk tolerance?

"Zero trust isn't just a technical evolution; it's a strategic imperative that enables agility, protection, and cost efficiency in an uncertain world."

— Jay Chaudhry, CEO, Founder, and Chair of Zscaler