The Future of Cybersecurity: Trust as Competitive Advantage

Accepted wisdom today is that there are two types of companies in the world: those that know they’ve been hacked and those that don’t. It’s not just a lift in cybersecurity spending that’s called for, however, but also a shift in thinking.

Trust will be the most important currency in the digital future—trust that companies will have to earn and work diligently to keep.
The cost of data breaches will reach US$2.1 trillion globally by 2019—nearly four times the cost in 2015.

Cyberattacks could cost up to $90 trillion in net global economic benefits by 2030 if cybersecurity doesn’t keep pace with growing threat levels.

Cyber insurance premiums could increase tenfold to $20 billion annually by 2025.

Cyberattacks are one of the top 10 global risks of highest concern for the next decade.

Companies are collaborating with a wider network of partners, embracing distributed systems, and meeting new demands for 24/7 operations.

But the bad guys are sharing intelligence, harnessing emerging technologies, and working round the clock as well—and companies are giving them plenty of weaknesses to exploit.

- 33% of companies today are prepared to prevent a worst-case attack.
- 25% treat cyber risk as a significant corporate risk.
- 80% fail to assess their customers and suppliers for cyber risk.

The ROI of Zero Trust

Perimeter security will not be enough. As interconnectivity increases so will the adoption of zero-trust networks, which place controls around data assets and increases visibility into how they are used across the digital ecosystem.

A Layered Approach

Companies that embrace trust as a competitive advantage will build robust security on three core tenets:

- **Prevention:** Evolving defensive strategies from security policies and educational approaches to access controls
- **Detection:** Deploying effective systems for the timely detection and notification of intrusions
- **Reaction:** Implementing incident response plans similar to those for other disaster recovery scenarios

They'll build security into their digital ecosystems at three levels:

1. **Secure products.** Security in all applications to protect data and transactions
2. **Secure operations.** Hardened systems, patch management, security monitoring, end-to-end incident handling, and a comprehensive cloud-operations security framework
3. **Secure companies.** A security-aware workforce, end-to-end physical security, and a thorough business continuity framework

Against Digital Armageddon

Experts warn that the worst-case scenario is a state of perpetual cybercrime and cyber warfare, vulnerable critical infrastructure, and trillions of dollars in losses. A collaborative approach will be critical to combatting this persistent global threat with implications not just for corporate and personal data but also strategy, supply chains, products, and physical operations.