Business Value of Zero Trust On A Page

*"Zero Trust is a cybersecurity **strategy** premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already **occurred** or will occur, and therefore, a user should **not** be granted access to sensitive information by a **single** verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be **continually** verified."*

- *NSTAC Report to the President on Zero Trust and Trusted Identity Management*

Zero Trust drives your selection and deployment of technology infrastructure, across the domains of identity, device, network, application, and data, and the cross-cutting areas of visibility and analytics, automation and orchestration, and governance.

Zero Trust does not have to be difficult, but it does require security and technology teams to establish partnerships with business stakeholders (which is largely the focus of this document).

Zero Trust improves security by ensuring that existing controls are operating as intended, as well as providing an organization with a continuous improvement program that further strengthens those controls.

Guiding Principles

*Beginning with the **End in Mind**:* This encourages one to establish a clear vision of the organization's desired direction and destination at the outset of the Zero Trust journey. Desired outcomes relevant to business value include reducing the cost of compliance, the financial impact of incidents, the complexity of IT and process debt, residual risk, and Total Cost of Ownership (TCO).

Breaches Happen. Acknowledging this fact allows for a shift in mindset from the impossible goal of being 100% secure, to the more achievable goal of instead being resilient.

Risk Management: Understanding the organization's risk appetite provides a threshold for acceptable risk.

Business Value

InfoSec investments are typically looked at in terms of TCO reduction, or as an enabler to driving business value. The following section provides fourteen different ways a Zero Trust initiative can deliver business value. Once you determine the applicable areas, you can quantify them appropriately, and incorporate them into the business case structure required by your organization.

- Cost Reduction and Optimization
- Operational Resilience
- Business Agility
- Facilitating Compliance
- Preserving Reputation and Brand Value
- IT Risk Reduction
- Secure Adoption of New Technology
- Accelerating Business Unit Integration (Merger & Acquisition)
- Better Leverage Existing Investments
- Improved Visibility & Analytics
- Improving User Experience

- Supporting Strategic Business Initiatives
- Reinventing Business Processes
- Business Value: Better Meet Prospective Customer Security Requirements