

FOUR ACTIONS EVERY SMB SHOULD TAKE REGARDING NETWORK SECURITY

→ In *Network Security for Small and Mid-Size Businesses*, Aberdeen noted that like virtually all modern organizations, most **small and mid-size businesses (SMBs)** today are built on the foundation of one essential technology: a reliable, high-performance **network**. Aberdeen’s research suggests four actions that every SMB should take with respect to network security.

| | |
|--------------------------|---|
| <input type="checkbox"/> | <p>Adopt a strategy for networking that delivers fast and reliable service, support for a dynamic mix of access and connectivity, and flexibility for future growth, while also addressing security risks, and sustaining requirements for regulatory compliance. For small and mid-size businesses to stay competitive and achieve their business objectives, SMB networks that may have initially been designed simply to support internal activities now need to adapt, integrate and keep up with the waves of disruptive changes in IT infrastructure that have rolled in over recent years – which include <i>mobility, social collaboration, virtualization</i> and <i>cloud computing</i>, among others. Once organizations get to even a modest size, this demands focus.</p> |
| <input type="checkbox"/> | <p>Establish a systematic, disciplined approach to network security. Aberdeen’s research shows that currently, the <i>consequences</i> of security incidents actually experienced by SMBs don’t align well with their <i>reasons for investing</i> in security in the first place. Security risks have become an issue both in the headlines and in executive boardrooms, and SMBs would be unwise to believe that they are somehow immune. Similarly, SMBs would be unwise to assume that they are not worth attacking – they are, and if not for their own resources, then as a link in an increasingly interconnected supply chain.</p> |
| <input type="checkbox"/> | <p>Make a build-or-buy decision about network security. Even if a given SMB has the resources (e.g., time, staff, budget) and capabilities (technical expertise) needed to implement traditional, on-premise network security solutions, is it really better off doing IT on its own – or would it be better off leveraging the expertise, scale and scope of a third-party service provider? This essential question is one part “can we,” and one part “should we.” Aberdeen’s research suggests 30% to 60% growth in network security services for SMBs, compared to low or no growth in traditional, in-house deployments.</p> |
| <input type="checkbox"/> | <p>Develop an appreciation of the costs of security-related business disruptions, data breaches and operational expenses of do-it-yourself network security – which may be higher than many SMBs may think. Aberdeen’s analysis estimates the median risk from unplanned downtime at about 0.8% of annual revenue, and the median risk from a data breach at 2.3%. As reported by SMBs, the cost advantage of network security services averaged about 50%.</p> |

→ **Read the full report:** *Network Security for Small and Mid-Size Businesses*, September 2015