The Cyber Security Leap: From Laggard to Leader

Executive Summary
Every security organization is looking for ways to achieve outsized results—to improve and expand on the value they deliver to the enterprises they support.

Rapidly evolving information security threats are a central challenge for organizations, which must continually strive to protect their proprietary information. How do corporations achieve better security performance while facing an ever-changing threat environment? Accenture collaborated with the Ponemon Institute LLC over a period of two years to research this critical issue, and found distinct similarities in companies that leapfrogged from a low to high level of security efficiency (average net change of 53 percent), compared with companies whose security performance remained static (average net change of two percent). The research outlines how Leapfrog organizations are more effective in addressing security across three key areas: **strategy**, **technology** and **governance**.

### STRATEGY

Leapfrog companies establish a security strategy that’s aligned with business objectives and focused on innovation to achieve a strong security posture. Innovation is a key driver in developing sustainable strategies that adapt to keep pace with evolving business needs to deliver effective security measures at scale, anywhere. Security is a priority supported with dedicated budget and programs, a strong ecosystem and a clear vision for moving forward. Static organizations, on the other hand, operate security under a veil of stealth, secrecy and underfunding. These organizations use regulations, not strategy, to drive their security requirements. They are more likely to focus on prevention rather than proactive detection or containment of threats.

### TECHNOLOGY

Leapfrog companies seek to develop security capabilities that enhance the user experience and productivity. To do this, they use technology to enable the organization’s digital uptake and improve their ability to counter advanced threats. They engage with new and disruptive technologies being embraced by the organization, instead of restricting or locking down the use of newer technologies. Static organizations are less proactive about changing their security approach when new or emerging threats occur.

### GOVERNANCE

Leapfrogging ahead in security effectiveness requires strong leadership and business alignment, with the correct governance measures in place. The Chief Information Security Officer (CISO) has the authority to define and manage the company’s security strategy, and has a direct communications channel established with the CEO and the board. Governance controls established across operations effectively measure results, assess the strategy to evolve the organization’s posture and realize the best use of resources. Within Static organizations, the CISO does not have the authority to set strategy, and does not have good communications access to the CEO and the board. Governance and controls are less effective within Static organizations, and they view security as a trade-off with employee productivity.

The Leapfrog organizations were able to make improvements over a relatively short, two year timeframe. Others looking to increase their security effectiveness can apply lessons learned from the Leapfrog companies to make a significant positive impact on their organizations’ security.