Client Context

- The diverse colleges, schools and institutes of a large R1 university were highly independent, limiting their use of enterprise IT to basic networking services, buying power for commodities, and some database and storage services
- The enterprise IT leader, responsible for a small security infrastructure group, asked Gartner to help improve its security services, with a focus on the group’s span of control

Business Challenges

- The university had executed its strategic plan to expand global presence but lacked sufficient insight on the risks of operating 24/7, including on servers outside the US
- The traditional IT “mindset” was tactical and decentralized; there was a concern that the university administration had no appetite for enterprise security governance or a Chief Information Security Officer (CISO)
- “Academic Freedom” was conflated with open access to computing resources and travel to hostile areas without protecting information on laptops and phones
- While the university had informal cooperation among its several CIOs, IT security issues were largely ignored, the appetite for security spending was low, and there was a lack of understanding and accountability for managing security issues and business threats

Approach/Differentiation

- Gartner used a comprehensive, collaborative approach to identify gaps in the university’s security posture related to strategy, process and technology, and link those gaps to the strategic objectives of university leadership and IT functions across the university
- Gartner demonstrated the business implications of the security gaps both within and outside of the control of the infrastructure group, making the case for improved security collaboration across the University

Benefits Achieved

- University leadership was able to build a consensus on implementing Gartner recommendations and expanding the influence of the central security group:
  - Creating a CISO position and hiring an individual with the ability to express security value
  - Contracting with a managed service provider to identify and block significant threats to the University’s network
  - Authorizing a program to identify and address security weaknesses that could disrupt university operations
  - Identifying information security thought leaders across the institution to communicate the importance of protecting university assets and participating in security governance efforts