IT Centralization at CWRU: The Path from IT to [U]Tech

THE IMPETUS

Members of the Board of Trustees were aware of newsworthy data breaches and hacks and had experience with security risks in their own businesses. A small group of representatives from Research Education Networking Information Sharing & Analysis Center (REN-ISAC), was engaged by Workman during the winter of 2014–2015 to conduct a small study of service risks and information technology practices at the university in response to increased security threats experienced across the globe. With this background of security awareness and growing tensions, the university president charged the newly recruited CIO and VP for Information Technology with consolidating all IT services to provide the best organizational structure in service of the university as a whole. The preliminary results confirmed that the silo structure exposed the university to security breaches that could be reduced with a central IT organization.

The president and board then commissioned a more expansive security audit by an external consulting agency to determine what if any changes should be made to improve vulnerability and strengthen efficiency. The auditor looked at three management centers (silos) at CWRU in-depth over several months. The CIO and the auditing agency presented the findings including several security issues recommending that servers across campus be put in protected data centers. The trustees weighed in with their experience of efforts to centralize IT operations. Discussions continued through 2015 about the pros and cons of centralization and the demands that such a transition would make. On January 5, 2016, the University President announced her decision to the full campus community that the university must make it a strategic priority to centralize all IT operations with all due speed. Four goals of centralization were stated at the outset:

1. Most importantly, reduce and effectively manage the risk profile of CWRU.

2. Ensure business continuity and disaster recovery readiness by leveraging best-practices across the university.
3. Improve the “IT experience” across all areas of the university.
4. Optimize the university’s investments in information technology.

Although the president recognized that such a transition in the university’s culture represented a high-risk effort, she knew the improved security and efficiency would make the risk worthwhile. By putting her endorsement into the initiative, she gave it full credibility and emphasized its priority.