Higher education leaders today face mounting pressure to compete for dwindling numbers of college applicants, account for learning outcomes, embrace technology innovation and disruption, and make key decisions regarding whether to move enterprise applications and infrastructure to the cloud. In the midst of this, there is an equally compelling need to ensure that the balance between information technology and information security is continually adjusted to provide adequate protection for the vast amount of information that is collected, processed, and stored across the institution. Objective assessments of security risks, needs, and considerations must be made clear to institutional leaders who make key decisions affecting strategic planning, budgeting, technology, and data security. The focus of this column is to highlight the advantages that can be gained by achieving that balance.

The Ongoing Challenge

With the explosive growth in information technology, IT leaders have had to scramble to keep pace, and in many cases, they are still in the midst of “catching up.” Given the fact that institutions are grappling with numerous security concerns and challenges, it’s safe to say that information security has also been obscured to varying degrees over the years. We believe that significant institutional vulnerabilities, combined with escalating security problems, require institutional leaders to respond more vigorously.

This belief is backed up by the EDUCAUSE annual look at the top IT issues in higher education. The relationship and balance between information security and IT priorities has made the Top 10 list for the last three years, appearing this year at both #8 (Developing mobile, cloud, and digital security policies that work for most of the institutional community) and #10 (Balancing agility, openness, and security). Without the direct buy-in and engagement of the rest of the campus—senior staff, administrative departments, and academic areas—efforts to decrease risks and prevent major security incidents may be significantly less effective.

A couple of years ago, before hiring Tammy Clark as Chief Information Security Officer (CISO), the University of Tampa engaged the services of a leading consulting firm to look at our security controls and to advise us on whether our security efforts were adequate or whether issues needed to be addressed. At the time, our IT area did not operate a formal information security program, we had limited staff time dedicated to information security within the IT organization, and none of the staff were certified or experienced in information security. The report we received hinted at multiple causes for concern. It was apparent that our institution was not making significant progress in addressing the breadth of security risks for today’s challenging security environment, even though we had made strides over the years within the IT organization to implement firewalls, virus protection, and other necessary restrictions.

The consulting firm advised the university to consider hiring a CISO to report outside of the IT organization in order to ensure a proper balance between IT priorities based on avoiding service disruptions or delays in implementing technology solutions and the critical need to proactively address security risks, compliance challenges, and threats to the integrity and confidentiality of institutional information.

During the interim process of deciding the reporting structure, we debated whether to place the CISO underneath the Chief Financial Officer (CFO), the Chief Information Officer (CIO), or the President. At the time, President Ronald Vaughn was dealing with the realization that the university faced substantial institutional information security risks. As he learned more about the IT area, suppliers, and vendors, the president concluded that the traditional IT industry response to security was inadequate and that the level of specialized information security knowledge at the university was fairly weak. Based on the consulting firm’s recommendations and the major issues in its report, he decided to have the CISO position report directly to the president (as does the CIO) to enable rapid progress on what he believed to be a critical institutional issue. Clark was brought onboard as CISO and as a member (along with the CIO) of the senior management team, to ensure the necessary breadth of perspective and influence to implement information security program goals across the institution. As Clark started working with the campus community and IT leadership, positive changes quickly improved the university’s overall security posture.
The Benefits of Effective Collaboration
A little over a year ago, we formalized the Office of Information Security as a separate organization. It now has four staff, all with information security specializations and industry certifications, to manage key information security initiatives. Clark and her team also manage information security technology solutions and have implemented a number of key components including network security solutions, vulnerability and penetration testing, forensics, data-loss prevention, data encryption, mobile/BYOD, and e-mail security solutions.

Clark and the CIO are charged with collaborating effectively for the good of the institution. The goals and objectives of both the CISO’s organization and the CIO’s organization must support institutional objectives, and both leaders are required to provide evidence that they are making a positive combined impact on a regular basis. Close collaboration between IT and information security staff at all levels allows this arrangement to work well. A major initiative that furthers this collaboration involves efforts to achieve ISO/IEC 27001:2013 compliance and certification, which includes effective implementation of controls that protect IT infrastructure, ensuring that business processes are adequately documented and assigning accountability to staff managing key IT and information security infrastructure pieces.

Last year, the new Office of Information Security managed a data-protection initiative that involved meetings and follow-up activities with all campus administrative departments and academic leaders to promote security awareness, to improve information-handling methods, to provide third-party oversight and contract reviews, to ensure compliance with regulatory requirements, and to help educate more staff and faculty through workshops, internal communiques, and (required) online security awareness training. Clark is conducting a formal risk assessment across the university to examine business processes and information handling, as well as vulnerabilities within the IT infrastructure. We’re also currently working on an ERP initiative led by the IT organization; the thoughtful consideration of security risks and controls is a key component of our discussions.

Many positive changes have been made in the past two years in both the IT and the information security organizations. For the most part, we are seeing a very complementary approach that validates the decision to have the CISO report outside of the IT organization. Although compromises often need to be made in the best interests of the institution, information security has quickly become an important consideration and one that we take into account every day. Our students, staff, and faculty are entitled to a high-quality educational and work environment, and they also deserve assurances that we are making our best efforts to protect their information.

Notes

Ronald L. Vaughn [rvaughn@ut.edu], President of the University of Tampa since January 1999 and holder of the Max H. Hollingsworth Chair of American Enterprise, previously served as Coordinator of the Department of Marketing, Director of the MBA program, Dean of the College of Business and Graduate Studies, and co-Chief Academic Officer. Tammy Clark [tclark@ut.edu] is Chief Information Security Officer (CISO) at the University of Tampa.

© 2015 Ronald L. Vaughn and Tammy Clark. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (http://creativecommons.org/licenses/by-nc-nd/4.0).