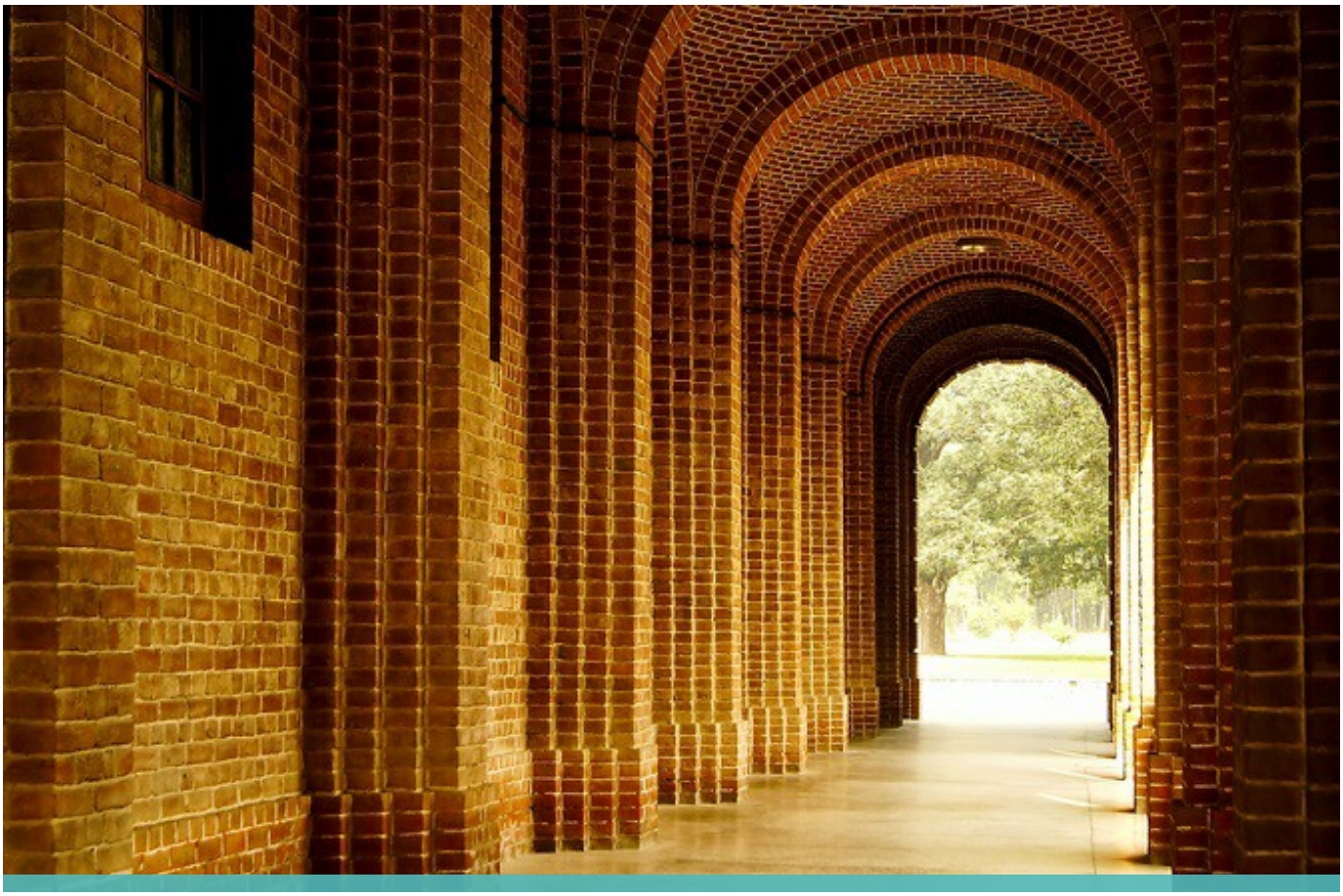
Pass or fail? Data privacy and cybersecurity risks in higher education



James J. Giszczak, Dominic A. Paluzzi | Tuesday, August 23, 2016

There is a long list of people who trust their sensitive financial, medical, and personal information to institutions of higher education – including donors, trustees, board members, alumni, students, parents, applicants, faculty, staff, researchers, medical patients, consumers, and vendors. And unfortunately, colleges and universities are becoming prime targets for cyberattacks because of the vast amount of data they collect and maintain from these sources.

In the first half of 2016, there was a 50 percent increase in higher education data breaches. These breaches cost the institution approximately $300 per record – not to mention the staggering loss in research grants and donations that stem from the loss of trust and confidence in the university.

Colleges and universities are also becoming targets because of the openness of their online communities. Network systems that have multiple points of access, with multiple departments and various users and third party vendors, can be a huge risk when it comes to data privacy.

In our latest white paper, McDonald Hopkins takes a look at the specific cyber risks for institutions of higher education, common causes and costs of a breach, and what preventative steps can be taken to prevent a breach from occurring.

Click here to download the white paper. For questions about data privacy in higher education, contact one of the attorneys listed below.

James J. Giszczak

Dominic A. Paluzzi