

Academic Institutions Face Increased Threat of Cyberattacks

July 19, 2013

American research universities typically structure their data and digital networks to be as accessible and open as possible to promote the open exchange and sharing of information. While an "open architecture" is excellent for academic freedom and the sharing and widespread dissemination of ideas, it also makes universities easy targets for cyberattacks. Around the country, universities and other centers of learning are being forced to increase security and restrict access to sensitive information such as intellectual property, research data, and personally identifiable information. The challenges of addressing data security on campus are much different than in government or in the private sector. It is difficult to provide a free flow of information while simultaneously placing access restrictions and user limits on data. Many universities are spending considerable time and money to rethink their approaches to information management. They are testing new methods and policies to attempt to share as much data as possible, while maintaining the most secure environment possible. Nonetheless, attacks and breaches continue to increase. A recent [New York Times article](#) reveals that several American universities have admitted to learning of break-ins or data breaches "much later, if ever, and that even after discovering the breaches they may not be able to tell what was taken" or compromised. A large number of recent attacks originated in China where hackers are skilled at masking their efforts and quickly identifying which data is valuable and which is not to minimize their footprint while breaching networks. Because university networks are accessed daily by thousands of students, professors, visitors and staff, the task of identifying an unauthorized user or detecting illicit behavior on the network is daunting. Some measures universities are taking include requiring all professors and staff to have their computers scrubbed for malware by a professional after returning from foreign travel, training researchers on federal law that prohibits them from taking certain types of data overseas, imposing access restrictions based on a need-to-know policy, and increasing budgets and staff significantly. All these measures present significant legal and internal governance challenges that should be addressed in an effective but legal manner.

Legal counsel should be involved at each step to ensure compliance with the law, and to help mitigate the privacy and intellectual freedom concerns of students and faculty.

Related Practices

[Cybersecurity and Privacy](#)

[Business Transactions](#)

[Intellectual Property](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.