The 12th Annual Dupont Summit on
Science, Technology, and Environmental Policy

Friday, December 6, 2019
The Historic Quaker Meetinghouse
2111 Florida Ave. NW, Washington DC

Title:

Caught in the Crosshairs of Cyber Aggression: Universities and Colleges are Prime Cyber Targets

By

Calvin Nobles, PhD
Cybersecurity Fellow
New America Think Tank
Calvin@CalvinNobles.com

Keni Galmai, Doctoral Candidate
University of Maryland Global Campus
Kgalmai18@gmail.com

Overview:

Colleges and universities are the nexus of education, the generators of innovative research and knowledge creation, and collaborative partners with industry and government stakeholders; nonetheless, higher education institutions vulnerability to cyber-attacks, data breaches, and ransomware attacks is a critical dark side. According to Demers, Harrington, Cianci, and Green (2017), in 2014, 30 universities and colleges experienced cybersecurity incidents in which 50,000 records were compromised. This highlights the gullibility of institutions of higher learning given the extensive amounts of data universities and colleges create, process, and store (Demers et al., 2017). With the increasing number of high-profile cybersecurity incidents occurring in the corporate and government domains, cyber-attacks on educational institutions have gone unnoticed. For example, in 2006, Ohio University experienced several cyber incidents, all stemming from various vulnerabilities within the institution's information technology infrastructure, which resulted in the compromising of 360,000 students and alumni records containing private and sensitive data (Keller, Williams, & Ewing, 2008). The exfiltrated data included social security numbers and other forms of confidential information. Fellow universities that felled victim to cyber-attacks, prior to 2010 were UCLA, Colorado University, the University of Virginia, the University of Iowa, the University of Missouri-Colombia, and the University of California-San Francisco, and the University of Kentucky (lost a thumb drive with personable identified information) (Keller, Williams, & Ewing, 2008). The abovementioned security incidents illustrate the susceptible nature colleges and universities accompanied by the prolonged cybersecurity incidents on the education industry; hence, keeping the institutions in the crosshairs of cyber-attacks.

Keller, Williams, and Ewing (2008) postulated the following:

> "Unlike for-profit corporations, for whom data loss can mean a hit to their bottom line, non-profit educational institutions have been historically less inclined to devote significant spending to secure their information or to upgrade and improve systems that collect and store a wealth of information" (p. 99).

In today's cyber attentive and fiducially focused environment, some colleges and universities have hired Chief Information Security Officers, implemented information security programs, and leveraged industry best practices to be compliant with federal regulations. The credit rating authority ranks the Education Sector as "medium" (McKenzie, 2019), and with the uptick attacks that are targeting colleges coupled with the fact that most data breaches are not reported, the scoring could potential be worse than "medium". Managing the cybersecurity risks in the higher education space is not an easy task; in fact, managing information technology infrastructure is a complicated function at most colleges.

More recent attacks occurred at Louisiana State University, Dartmouth, St. Michael's College, Wesleyan College, Coastal Carolina College, and Bowling Green State University ("Big Phish, 2017). The 2017 Verizon Data's Breach Investigations Report indicated that were 455 cybersecurity incidents in the educational industry, which resulted in 73 cases of data disclosures (Polyakov, 2017). Researchers and practitioners emphasize that (a) malware, (b) phishing, (c) network attacks, (d) social engineering, and (e) peer-to-peer information spillage daily threats for most colleges and universities (Demers et al., 2017). The average cost of compromised records in the education sector is $246 compared to other industries at $221, which highlights the increasing liability affronted by colleges and universities (Demers et al., 2017).

Currently, 41% of universities have hired a Chief Information Security Officer, which is a 7% increase from 2017 (Brown, 2019). However, 85% of institutions require information security training for faculty and staff; less than half mandate the same training for students (Brown, 2017). The lack of mandatory information security training for students is a significant risk and self-induced vulnerability that cybercriminals will exploit to gain access to confidential and sensitive data. Other insights such as (a) 71% universities follow-up on information security metrics, (b) 76% of institutions have executed an information security assessment, and (c) 25% of colleges have conducted risk assessments on their cloud service providers and third-party partners (Brown, 2019). Monrad (2016) opines that universities need to undergo a security reeducation specifically targeting contemporary attack vectors such as (a) ransomware attacks, (b) data breaches, and (c) social engineering attacks. The reeducation needs to include training for students who accounts for most of the personnel using the network.

College and universities are prime targets because of the large student population and the sensitive data stored within the systems of the institutions. Additionally, colleges and universities enroll 20.4 million students and 1.6 faculty members (Mello, 2018) this is an enormous footprint and what makes the education sector attractive to cybercriminals. Between 2005-2013, data breaches wreaked havoc on higher education institutions; however, in 2014, data breaches dropped significantly according to the reporting (Mellos, 2018). Given the reputational damage and embarrassment from a data breach, many organizations to include colleges are not reporting data breaches. Another factor is the lack of a central reporting repository of cybersecurity incidents for higher education institutions accompanied by the regulatory directives to mandate that all colleges and universities report any security incident to the broadest audience possible.

McKenzie (2019) reports that 11% of security incidents are due to espionage occurring at institutions of higher learning. Another alarming statistic is that 70% of colleges received a fail rate on application security (Kuchler, 2015), cybercriminals can inject scripts into software code that is not secure to perform malicious actions and functions to impact information security, data security, and privacy adversely. Symantec reports that the education sector was responsible for 10% of all data breaches in 2014 (Kuchler, 2015).

In a study by Mello (2018), the findings indicated that cybercriminals target highly paid faculty members along with students from affluent families, and universities with more financial capability were targeted over higher educational institutions with less fiscal capacity. This is indicative of cybercriminals conducting intelligence on students, faculty, and institutions before executing malicious activities. Institutions that do not mandate information security training for students could potentially experience an uptick cybersecurity incidents that specifically target students. The open nature of universities, number of student-owned devices, lack of security enforcement, and numerous access points (Monrad, 2016) make it incredibly challenging to remediate without changing the cybersecurity culture at colleges and universities.

The purpose of this research is to call attention to the cybersecurity problems at universities and colleges, the lack of security preparedness, and the abundance of cyber targets associated with the institutions. Higher education institutions remain in the crosshairs as prime cyber targets because of their sheer nature and existence and the students' information security awareness incompetence. Colleges and universities can implement defensive measures to mitigate the existing cyber threats; yet, it requires a constant effort to achieve the level of cybersecurity resiliency to prevent (a) data breaches, (b) ransomware attacks, and (c) cyber-attacks.

References

Big Phish on Campus: The cybercrime wave hitting colleges. (2017, May 11). Retrieved from https://www.threatmetrix.com/digital-identity-blog/cybercrime/big-phish-campus-cybercrime-colleges/

Brown, M. (2019, June 26). With lingering security gaps, higher ed student data breaches remain a concern. EdTechMagazine.com. Retrieved from https://edtechmagazine.com/higher/article/2019/06/lingering-security-gaps-higher-ed-student-data-breaches-remain-concern

Demers, G., Harrington, S., Cianci, M., & Green, N. (2017). Protecting colleges & universities against real losses in a virtual world, 33 J. Marshall J. Info. Tech. & Privacy L. 101 (2017). *The John Marshall Journal of Information Technology & Privacy Law*, *33*(2), 3.

Kellers, J., Hill, M., and Ewing, S. (2008). Identity theft and data loss on campus— Minimizing and addressing risk. University Risk Management and Insurance Association Journal. Retrieved from http://stg.saul.com/sites/default/files/1147_pdf_1618.pdf

Kuchler, Hannah. (2015, November 30). Universities steel themselves for wave of cyber-attacks. *Financial Times.Gale Academic One file.* Retrieved from https://link.gale.com/apps/doc/A435991821/AONE?u=temple_main&sid=AONE&xid=8989539.Accessed 6 Nov. 2019.

McKenzie, L. (2019, May 21). Colleges face growing cybersecurity threat. Insidehighered.com. Retrieved from https://www.insidehighered.com/quicktakes/2019/05/21/colleges-face-growing-cybersecurity-threat

Mello, S. (2018). Data breaches in higher education institutions. Retrieved from https://scholars.unh.edu/cgi/viewcontent.cgi?article=1407&context=honors

Monrad, J. (2019, August 27). Universities fall into the crosshairs of cyber attackers. Infosecurity-Magazine.com. Retrieved from https://www.infosecurity-magazine.com/opinions/universities-attackers/

Polyakov, M. (2017, May 21). What cyber threats do higher education institutions face? Forbes.com. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2017/08/21/what-cyberthreats-do-higher-education-institutions-face/#6c0941a8640d