International Journal on New Trends in Education and Their Implications
April 2019 Volume: 10 Issue: 2 ISSN 1309-6249

HIGHER EDUCATION'S CYBER SECURITY: LEADERSHIP ISSUES, CHALLENGES AND THE FUTURE

Prof. Dr. G. David Gearhart
University of Arkansas- USA

Prof. Dr. Michael D. Abbiatti
Western Interstate Commission for Higher Education- USA

Prof. Dr. Michael T. Miller
University of Arkansas- USA

Abstract
Cyber security is a major concern in all industries, but is particularly of concern to leaders in higher education. The academy's housing of major biographical and financial data, in addition to data related to research and development of new technologies, makes colleges and universities susceptible to cyber attacks. The coordination, implementation, and direction of cyber security has subeequently grown to be a major concern on college campuses, with the campus leader or president typically having ultimate authority over cyber security strategy. Using a research-team developed survey instrument that was administered to 150 college presidents, the current study sought to determine the extent of senior college leaders involvement in cyber security. Study findings revealed that the authority for cyber security strategy was predominantly distributed to the senior information or business officer, that there are major concerns about the safety of data related to financial, student, faculty, and donor affairs, and that about half of college leaders talk about cyber security related issues 2-6 times per week. Further research that explores how decisions are made about cyber security priorities, as well as how to best provide training for better cyber security decision-making were recommended.

Keywords: Higher Education, Cyber Security, College Presidents, Technology in Higher Education, Decision- Making.

INTRODUCTION

Higher education has grown increasingly complex, and the range of issues that college leaders face has changed significantly in the past two decades (Ruscio, 2017; Kezar, 2010). A particular challenge has been the evolution, use, and management of technology (Mungo & Clough, 1993). Evolving from providing photocopy services and early computer labs, institutions now rely on complex information system structures to manage the entirety of their campus' operations. These functions include everything from applications that contain sensitive and confidential information to financial billings, accounts receivable, human resources data, classroom and academic information, and even coded electronic entry management systems for room and building access. There is no element of the contemporary university that is immune from the pervasive growth and infiltration of technology (Daly, 2012).

Within the past 20 years, the issue of technology safety has become a significant issue that college leaders, especially presidents, have had to become proficient with. Initial concerns about 'hacking' email have grown to be a significant, comprehensive data protection system concern. As a society, Ashford (2018) estimated that over $1 million is lost in cyber related crime every minute, and that nearly 2,000 people are victim of cyber related crime during that same time frame.

In the academy, Goral (2014) noted that perimeter security is no longer an issue, cyber security is a system and structure that must exist within systems. He categorized two types of cyber security criminals: those who are part of organized criminal gangs, including foreign bodies, and those who

focus on long-term 'sieges,' attacking a campus over a long period of time. He also reinforced the idea that universities, particularly research universities, are a prime target for cyber criminal activity.

The result of cyber crime has a strong financial element, as criminals look to find access to money that they can syphon to their own accounts, but also knowledge related data that can impact technology transfer and copy and patent filing. Fishman, Clark, and Grama (2018) also identified the extreme peril and risk for cyber security for a campus in terms of reputational damage and operational damage. Their report, part of the Deloitte Center for Higher Education Excellence's work, particularly called for strong higher education leadership to combat cyber criminal activity, and that this leadership, at the highest level, must both coordinate activities, but also stress the need for communication between campus agencies and offices and keeping cyber welfare at the forefront of campus actions.

Due to the comprehensive nature of higher education's services and span of offerings, they are of particular risk to cyber related crime. Multiple users of hardware and software (both internal and external to campus), a broad array of sensitive data ranging from Social Security numbers to credit card and bank accounts, and a global presence all add to the challenges facing colleges and universities. Set against this backdrop are college leaders who until very recently followed a traditionally academic focused career path to assume a presidency (Braswell, 2006). Expertise in an academic discipline, however, has rarely proven to be an adequate training for handling the complexity of roles of the contemporary college president, including, but certainly not limited to, cyber security. Therefore, the purpose for conducting the current study was to determine the extent of senior college leaders involvement in cyber security.

BACKGROUND OF THE STUDY

The American college presidency has evolved dramatically along with the structure, function, use, and composition of the college and university (Tolliver & Murry, 2017). Early college presidents were involved in every aspect of the institution's management, whether purchasing food for students, directly hiring faculty members to teach, and even collecting cash tuition payments from students and their parents. The evolution of the institution, including the implementation of academic departments, has led to a greater level of sophistication in the presidential role, with some considering the position very similar to that of a political figure. The position has even been described as one of the most stressful, complex, and difficult of any senior executive position (Thomason, 2018).

With the evolution of the college president position, a variety of skills and abilities have become more prominent than in past decades (Morris, 2017). The contemporary college president provides leadership to complex systems that involve a broad array of state and federal rule and regulation compliance, a pace and growth of knowledge that has never before been experienced, management and solicitation of a more diverse revenue stream, and calls for accountability from a wider, more complex, and geographically diverse group of stakeholders (Cook, 2012).

One result of the changing responsibilities facing college presidents is their increasingly diverse preparation and career progression prior to assuming the presidential role. Braswell (2006) noted this diversity of career experiences, citing the rising number of college presidents coming from public service, the business sector, the military, and increasingly, non-academic backgrounds from within the academy. This broad labor preparation for these positions has been augmented by a growing number of professional preparation programs for college presidents, some of them sponsored by academic or professional associations and some of them sponsored by colleges and universities. An increasingly common curricular component within these training programs has become technology management and cyber security. The Western Interstate Commission on Higher Education, as well as Homeland Security, have similarly begun working to support higher education leaders in managing their cyber security efforts.

In addition to administrative training programs, multiple institutions have begun academic programs related to cyber security. Arizona State University, the University of Arizona, Syracuse, Georgetown, and the University of California-Berkeley all offer formal degree programs, for example, in cyber security.

Some college leaders, however, still find the process and attempts to effectively manage cyber security to be a massive and expensive undertaking. Daub (2018) reported that in response to these complexity and cost issues, a consortium of leading research universities created a partnership to better manage their cyber security policies and platforms. Led by Northwestern, Purdue, Nebraska, Indiana, and Rutgers, this partnership (OmniSO) has come to be seen as a leading example of pooling expertise and resources to combat the growing challenge of cyber security.

RESEARCH METHODS

Due to the emerging nature of cyber security in higher education, a descriptive research design was determined to be appropriate to address the purpose for conducting the study. A research-team survey instrument was developed based on concerns, ideas, and issues presented in both the academic and professional literature in cyber security. This 8 item survey instrument was distributed to a panel of experts for review, with clarifications identified and made to the instrument to assure face value validity. Additionally, review of the instrument for face validity was conducted by professional staff associated with a leading national association located in the mountain-west United States. Following these reviews, changes and modifications to wording were completed.

The first 7 survey questions were designed to understand who was completing the survey and general impressions and practices within higher education's senior leadership regarding cyber security. The last question contained 10 statements, requesting survey respondents to rate their agreement with each on a 5-point Likert-type scale (ranging from 1=Strongly Disagree progressively to 5=Strongly Agree).

The sample included 150 randomly chosen college presidents. Using an on-line available listing of US colleges and universities of approximately 3,000, 150 institutions were selected for inclusion in the study. Following the identification of the institution, each was manually explored online to identify who was the institution's campus leader was (chancellor or president title) and the individual's email address. Three of the institutions did not provide a name for the senior leader role, and these were replaced in the sample. Additionally, the institutions with interim leadership were removed from the sample.

The survey instrument was distributed electronically in the winter of 2019. Four email reminders were used to provide those identified in the sample ample opportunity to participate in the study.

FINDINGS

A total of 16 surveys were completed and deemed usable following the initial survey distribution, with 3, 11, 4, and 5 surveys completed following each email reminder. The total response was 39 usable surveys for a 26% response rate. This response rate was deemed appropriate for the descriptive nature of the study and the online format of survey distribution.

Despite the survey being addressed to the campus president, the majority of those completing the survey held support positions to the president (n=13; 38.2%), although a near-equal percentage of presidents completed the survey themselves (n=11; 32.4%). As shown in Table 1, several chief/senior information officers also completed the survey (n=6; 17.6%), as did several representatives of a systems office (n=4; 11.8%). Nearly all of these individuals indicated that cyber

security is an extremely or very important institutional priority (*n*=33; 97.19%), and that their campuses prioritize work on cyber security (*n*=32; 96.9%).

Table 1: Descriptive Information from Respondents

Question area	#	%
Role of Respondent		
Support position to Chancellor or CIO	13	38.3
Chancellor/President of campus	11	32.4
Chief/Senior Information Officer	6	17.6
Higher education systems level leader	4	11.8
To what extent is cyber security an institutional priority		
Extremely important	14	41.2
Very important	19	55.9
Moderately important	1	2.9
To what extent does your campus prioritize work on cyber security		
Extremely important	14	42.4
Very important	18	54.5
Moderately important	1	3
How often is cyber security discussed with senior institutional leaders		
Daily	1	3
Once a week	13	39.4
2-3 times per week	9	27.3
4-6 times per week	6	18.2
Once a month	4	12.1
Should more time be devoted to cyber security		
Yes	20	60.6
No	13	39.4
Primary responsibility for assuring that CS is on the institutional leadership's agenda		
CIO	16	48.5
Business Affairs/Admin Services	15	45.5
Academic Affairs	1	3
Campus leader (president)	1	3
Primary areas of concern for cyber security		
Financial data	30	76.9
Student issues/data	29	74.4
Faculty and employee data	27	69.2
Donor and philanthropic data	22	56.4
Institutional records	20	51.3

Also shown in Table 1, over half of the respondents (*n*=20; 60.6%) indicated that more time should be spent on cyber security efforts, and the majority also indicated that the chief/senior information officer (*n*=16; 48.5%) or senior business affairs/administration officer (*n*=15; 45.5%) should lead these efforts. These respondents also indicated that they discuss cyber security with the senior leadership team at their institutions on a regular basis, including 39.4% (*n*=13) who discuss cyber

security once per week, 27.3% 2-3 times per week, and 18.2% 4-6 times per week. The most common concerns for cyber security issues were financial data (*n*=30; 76.9%) and student issues and data (*n*=29; 74.4%).

Table 2: Perceptions of Cyber Security Issues

	$\bar{x}$	Min	Max	SD	Var
CS issues fall within the domain of the CIO	4.85	4.0	5.0	.36	.13
Cyber security is an issue that must be dealt with	4.58	4.0	5.0	.49	.24
Targeted training should be provided to presidents	3.76	2.0	5.0	.70	.49
CS training should be provided on-demand, online	3.55	2.0	5.0	.86	.73
CS threatens the future of higher education	3.45	2.0	5.0	.89	.79
More training is needed for college leaders about CS	3.45	1.0	5.0	.89	.79
CS can be effectively managed by HIED systems	3.36	2.0	5.0	.98	.96
President have primary responsibility for CS	3.15	1.0	5.0	1.21	1.46
CS training should be coordinated by associations	2.94	1.0	5.0	.95	.91

Members of the sample were also asked to rate their level of agreement with a series of statements about the practice of cyber security on their campuses. These 9 statements were all developed based on both the emerging academic and professional literature on cyber security. On a 1-to-5 Likert-type scale (1=Strongly disagree progressing to 5=Strongly agree) respondents agreed most strongly that cyber security issues fall within the domain of the senior/chief information officer ($\bar{x}$ = 4.85; SD .36), and that cyber security issues are indeed an important issue that must be dealt with by higher education institutions ($\bar{x}$ = 4.58; SD .49). These same respondents agreed the least strongly with having training for cyber security being coordinated by professional associations ($\bar{x}$ = 2.94; SD .95) and that the college president should have primary responsibility for cyber security ($\bar{x}$ = 3.15; SD 1.21).

DISCUSSION

These descriptive findings offer significant insights into how cyber security is viewed on campus. They generally point in the direction of understanding how important cyber security is, but also that the responsibility for such protections are delegated to a particular office on campus. Some of the discrepancy in the response as to who should have responsibility for cyber security may be in the nuanced perspective of how different colleges and universities are organized. For example, information systems and computing might be under business affairs or administrative operations at one university, and might be a direct report to the campus president at another institution. The clearest part of the response, though, is that the president, while responsible for all aspects of the institution and its operation, is seen as an individual who delegates responsibility for the cyber security operations to the most appropriate, perhaps knowledgeable, individual on staff.

Respondents reinforced their perspectives about who should be responsible for cyber security in their ratings of various issues. By agreeing most strongly with assigning cyber security to the CIO position, there was a reinforcement of who should be responsible within the campus structure for this work. There was also some ambivalence about where and how professional development training should occur, with moderate agreement with the included statements about the provision of this training, be it online or coordinated by professional associations. If professional associations, however, do not take the leadership of providing cyber security related training, there may be a lack of leadership in creating forward thinking training programs that bring higher education leaders into the continued conversation of protecting their campus' data.

There is a lack of scholarly literature describing and inferring the major issues and response strategies for the cyber security of higher education. As a growing field, and as a growing concern for college administrators, there must be a concentrated and immediate strategic direction forged for how this research and literature are developed and shared. By creating a well-documented, reasoned, and logical approach to better understanding the multiple-dimensions to cyber security, the academy can become better prepared to face the growing assault on the big data that they protect.

BIODATA AND CONTACT ADDRESSES OF AUTHORS

G. David Gearhart is a Professor of Higher Education and Chancellor Emeritus of the University of Arkansas. He currently directs the National Lab for the Study of the College President and serves as editor of the Journal for Research on the College President.

G. David Gearhart
College of Education and Health Professions
University of Arkansas, Fayetteville, AR 72701- USA
E. Mail: gdgearh@uark.edu

Michael D. Abbiatti is the Executive Director of the Western Cooperative for Educational Technologies and Vice President of the Western Interstate Commission for Higher Education.

3035 Center Green Drive, Suite 200, Boulder, CO 803301- USA
E. Mail: mabbiatti@wiche.edu

Michael T. Miller is a Professor of Higher Education and Dean of the College of Education and Health Professions at the University of Arkansas. His address is Graduate Education Building 324, College of Education and Health Professions, University of Arkansas, Fayetteville, AR 72701,

Michael D. Abbiatti (Corresponding author)
324 Graduate Education Building
College of Education and Health Professions
University of Arkansas- USA
Fayetteville, AR 72701
E. Mail: mtmille@uark.edu

REFERENCES

Ashford, W. (2018, August 21). Online crime costs more than $1m a minute. *Computer Weekly*, retrieved online at www.computerweekly.com/news/25244729/Online-crime-costs-more-than-1m-a-minute?

Braswell, K. H. (2006). *A grounded theory describing the process of executive succession at Middle State University*. Unpublished doctoral dissertation, University of Arkansas, Fayetteville, AR.

Cook, B. J. (2012). The American college president study: Key findings and takeaways. *The Presidency, American Council on Education*, retrieved online at acenet.edu/the-presidency/columns-and-features/Pages/The-American-Colelge-President-Study.aspx

Daly, J. (2012, November 12). Technology's pervasive impact on higher education. *EdTech Focus on Higher Education*, retrieved online at https://edtechmagazine.com/higher/article/2012/11/technologys-pervasive-impact-higher-education-infographic.

Daub, C. (2018, March 31). Five universities join hands to improve cyber security on college campuses. *The Daily Pennsylvanian*, retrieved online at www.thedp.com/article/2018/03/upenn-penn-philadelphia-privacy-security-breach-private-information-threat-detection-norrthwestern

Fishman, T. D., Clark, C., & Grama, J. L. (2018, February 22). Evaluating cybersecurity on the higher education leadership agenda. *Deloitte Insights*, retrieved online at www2.deloitte.com/insights/us/en/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html

Goral, T. (2014, March 31). Keeping cyber attacks at bay. *University Business*, retrieved online at www.universitybusiness.com/article/keeping-cyber-attacks-bay

Kezar, A. (2010). Change in higher education: Not enough or too much. *Change, 41*(6), 18-23.

Morris, A. (2017). Challenges and opportunities facing the community college president in the 21st century. *Journal of Research on the College President, 1*, 2-8.

Mungo, P., & Clough, B. (1993). *Approaching zero: The extraordinary underworld of hackers, phreakers, virus writers, and keyboard criminals*. New York, NY: Random House.

Ruscio, K. P. (2017, March/April). The role of the president in today's university. *Change, 49*(2), 26-29.

Thomason, A. (2018, May 1). Is the college president 'the toughest job in the nation?' *Chronicle of Higher Education*, retrieved online at chronicle.com/article/Is-College-President-the/243289

Tolliver, III, D. V., & Murry, J. W., Jr. (2017). Management skills for the contemporary college president: A critical review. *Journal of Research on the College President, 1*, 9-17.